

10/509872

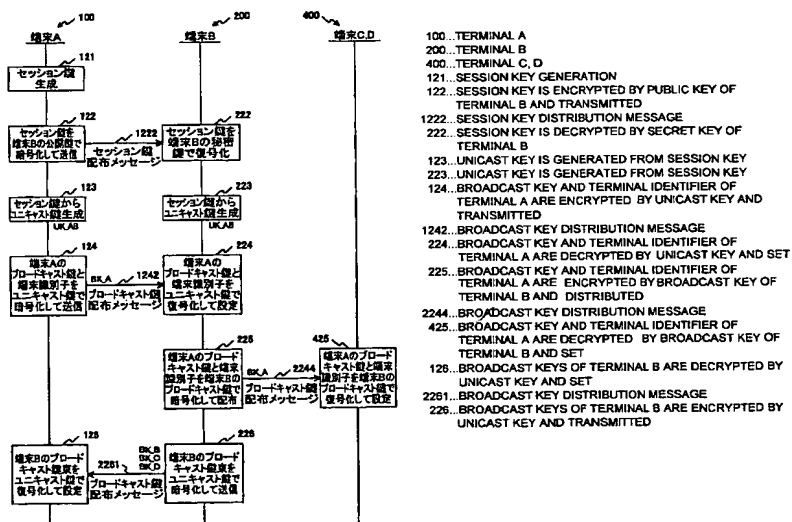


## PCT

(10) 国際公開番号  
**WO 2004/071006 A1**

- 〔統葉有〕

(54) 発明の名称: ブロードキャスト暗号鍵配布システム



〔統葉有〕

(57) 要約: 無線アドホック通信システムにおける各端末は暗号鍵管理リストテーブル660を備える。この暗号鍵管理リストテーブル660では、MACアドレス等の端末識別子661に関連付けられて、その端末識別子661により識別される端末との間のユニキャスト通信に用いられるユニキャスト暗号鍵662およびその端末識別子661により識別される端末がブロードキャスト通信を行う際に用いられるブロードキャスト暗号鍵663が保持される。これにより、ブロードキャスト通信を行う

**WO 2004/071006 A1**



SK, SL, SY, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ,  
VC, VN, YU, ZA, ZM, ZW.

- (84) 指定国 (表示のない限り、全ての種類の広域保護が可能): ARIPO (BW, GH, GM, KE, LS, MW, MZ, SD, SL, SZ, TZ, UG, ZM, ZW), ユーラシア (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), ヨーロッパ (AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HU, IE, IT, LU, MC, NL, PT, RO, SE, SI, SK, TR), OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, ML, MR, NE, SN, TD, TG).

添付公開書類:

- 国際調査報告書
- 補正書

2文字コード及び他の略語については、定期発行される各PCTガゼットの巻頭に掲載されている「コードと略語のガイダンスノート」を参照。

## 明 細 書

次に示すように国際調査機関が作成した。

5       ブロードキャスト暗号鍵配布システム

## 技術分野

本発明は、無線アドホック通信システムに関し、特に端末毎に異なる  
ブロードキャスト暗号鍵によりブロードキャストフレームを暗号化して  
10   秘匿性を保つ無線アドホック通信システム、当該システムにおける端末、  
および、これらにおける処理方法ならびに当該方法をコンピュータ（端  
末）に実行させるプログラムに関する。

## 背景技術

15    電子機器の小型化、高性能化が進み、簡単に持ち運び利用することが  
可能となったことから、必要になったその場で端末をネットワークに接  
続し、通信を可能とする環境が求められている。その一つとして、必要  
に応じて一時的に構築されるネットワーク、すなわち無線アドホックネ  
ットワーク技術の開発が進められている。この無線アドホックネットワ  
20   ークでは、特定のアクセスポイントを設けることなく、各端末（例えば、  
コンピュータ、携帯情報端末（PDA: Personal Digital Assistance）、携帯電話等）が自律分散して相互に接  
続される。このような無線アドホック通信システムにおいても、重要な  
情報の送受やプライベートなやりとりが第三者に傍受されることなく安  
25   心して行えるように暗号化等による秘匿性が求められている。

一般に、通信内容を暗号化するためには、暗号化および復号化の両者

で同じ共通鍵を用いる共通鍵暗号方式と、暗号化には公開鍵を用いて復号化には秘密鍵を用いる公開鍵暗号方式の二つの暗号方式が用いられている。共通鍵暗号方式は、暗号化および復号化を高速に行うことが可能であるが、通信の当事者同士が事前に何らかの方法で共通鍵を共有しておく必要がある。一方、公開鍵暗号方式は、共通鍵暗号方式に比べると処理が遅いが、当事者間同士で鍵を共有する必要がないという利点がある。そこで、共通鍵暗号の高速性と公開鍵暗号の利便性を組み合わせるハイブリッド方式が一般的に用いられている。具体的には、公開鍵暗号方式を用いて共通鍵を暗号化して送信し、当事者間で共有した共通鍵で  
5 実際の通信データの暗号化を行うことになる。

この通信データの暗号化のための共通鍵は、用途に応じてユニキャスト暗号鍵とブロードキャスト暗号鍵とに分類される。ユニキャスト暗号鍵は、二つの端末間のユニキャスト通信において用いられるものであり、その二つの端末以外には知らされない共通鍵である。一方、ブロードキャスト暗号鍵は、ある端末からのブロードキャスト通信を各端末において復号化するために用いられるものであり、ブロードキャスト通信にかかわる全ての端末間で共有される共通鍵である。従って、ブロードキャスト暗号鍵は、ユニキャスト暗号鍵と比較して一般に、秘匿性を維持することが難しくなる。

そのため、従来の通信システムにおいては、ブロードキャスト暗号鍵はネットワーク上の特定の装置において一元管理され、ブロードキャストグループにおけるブロードキャスト暗号鍵の秘匿性が図られている。例えば、モバイルデバイスに対してネットワーク所有者であるワイヤレスキャリアがブロードキャスト暗号鍵を予め設定しておくことにより、  
20 ブロードキャストメッセージを暗号化する技術が提案されている（例えば、特表 2002-501334 号公報（図 1）参照。）。  
25

従来の通信システムではブロードキャスト暗号鍵は一元管理されているが、無線アドホック通信システムにおいては端末は常に移動し、端末の参入および脱退が頻繁に行われ、ブロードキャストグループを構成する端末を固定することができない。また、無線媒体の性質上、そのような一元管理を行う装置への通信路が常に確保されているとは限らないため、一元管理に適さない。

そこで、本発明の目的は、無線アドホック通信システムにおいて、ブロードキャスト暗号鍵の管理を自律分散して行うことにある。特に、本発明は、ネットワークを構成する全ての無線端末が管理情報（例えば、

#### 発明の開示

上記課題を解決するために本発明の請求項 1 記載の無線アドホック通信システムは、複数の端末により構成される無線アドホック通信システムであって、ブロードキャストフレームのペイロードを暗号化して当該ブロードキャストフレームを送信する第 1 の端末と、上記ブロードキャストフレームを受信して当該ブロードキャストフレームのペイロードを復号する第 2 の端末とを具備し、上記第 1 の端末は上記第 1 の端末のブロードキャスト暗号鍵により上記ブロードキャストフレームのペイロードを暗号化し、上記第 2 の端末は上記第 1 の端末のブロードキャスト暗号鍵により上記ブロードキャストフレームのペイロードを復号する。これにより、端末毎にブロードキャスト暗号鍵を自律分散して設定可能にするという作用をもたらす。

また、本発明の請求項 2 記載の無線アドホック通信システムは、請求項 1 記載の無線アドホック通信システムにおいて、上記第 2 の端末が、上記第 1 の端末の端末識別子と上記第 1 の端末のブロードキャスト暗号

鍵との組からなる暗号鍵管理リストを少なくとも有する暗号鍵管理リストテーブルと、受信したブロードキャストフレームの始点端末識別子に含まれる上記第1の端末の端末識別子により上記暗号鍵管理リストテーブルを検索して対応する上記第1の端末のブロードキャスト暗号鍵を抽出する手段と、抽出された上記第1の端末のブロードキャスト暗号鍵により上記ブロードキャストフレームのペイロードを復号する手段とを備える。これにより、ブロードキャストフレームの始点端末識別子に応じてブロードキャスト暗号鍵を選択可能にするという作用をもたらす。

- また、本発明の請求項3記載の無線アドホック通信システムは、請求項8記載の無線アドホック通信システムにおいて、上記第1の端末が、上記第1の端末のブロードキャスト暗号鍵を保持する生成鍵テーブルと、ブロードキャストフレームのペイロードを上記生成鍵テーブルに保持された上記第1の端末のブロードキャスト暗号鍵により暗号化する手段と、暗号化された上記ブロードキャストフレームを送信する手段とを備える。
- これにより、ブロードキャスト通信を行う際に端末毎に異なるブロードキャスト暗号鍵によりブロードキャストフレームを暗号化することを可能にするという作用をもたらす。

- また、本発明の請求項4記載の端末は、他の端末の端末識別子と上記他の端末のブロードキャスト暗号鍵との組からなる暗号鍵管理リストを少なくとも一つ有する暗号鍵管理リストテーブルと、受信したブロードキャストフレームの始点端末識別子を含む上記暗号鍵管理リストを上記暗号鍵管理リストテーブルから検索して対応する上記ブロードキャスト暗号鍵を抽出する手段と、抽出された上記ブロードキャスト暗号鍵により上記ブロードキャストフレームのペイロードを復号する手段とを具備する。これにより、端末毎にブロードキャスト暗号鍵を自律分散して設定しておいて、ブロードキャストフレームの始点端末識別子に応じてブ

ロードキャスト暗号鍵を選択可能にするという作用をもたらす。

また、本発明の請求項 5 記載の端末は、他の端末の端末識別子に対応して上記他の端末との間のユニキャスト暗号鍵および上記他の端末のブロードキャスト暗号鍵を保持する暗号鍵管理リストを少なくとも一つ有する暗号鍵管理リストテーブルと、受信したフレームの終点端末識別子がブロードキャストアドレスであれば当該フレームの始点端末識別子を含む上記暗号鍵管理リストを上記暗号鍵管理リストテーブルから検索して対応する上記ブロードキャスト暗号鍵を暗号鍵として抽出し、上記受信したフレームの終点端末識別子がブロードキャストアドレス以外であれば当該フレームの始点端末識別子を含む上記暗号鍵管理リストを上記暗号鍵管理リストテーブルから検索して対応する上記ユニキャスト暗号鍵を上記暗号鍵として抽出する手段と、抽出された上記暗号鍵により上記フレームのペイロードを復号する手段とを具備する。これにより、受信したフレームの終点端末識別子に応じてブロードキャスト暗号鍵およびユニキャスト暗号鍵を使い分けることを可能にするという作用をもたらす。

また、本発明の請求項 6 記載の端末は、自端末のブロードキャスト暗号鍵を保持する生成鍵テーブルと、ブロードキャストフレームのペイロードを上記ブロードキャスト暗号鍵により暗号化する手段と、暗号化された上記ブロードキャストフレームを送信する手段とを具備する。これにより、ブロードキャスト通信を行う際に端末毎に異なるブロードキャスト暗号鍵によりブロードキャストフレームを暗号化することを可能にするという作用をもたらす。

また、本発明の請求項 7 記載の端末は、自端末のブロードキャスト暗号鍵を保持する生成鍵テーブルと、他の端末の端末識別子に対応して上記他の端末との間のユニキャスト暗号鍵を保持する暗号鍵管理リストを

少なくとも一つ有する暗号鍵管理リストテーブルと、送信しようとするフレームがブロードキャストフレームであれば上記生成鍵テーブルの上記ブロードキャスト暗号鍵により上記ブロードキャストフレームのペイロードを暗号化し、送信しようとする上記フレームがユニキャストフレームであれば当該ユニキャストフレームの終点端末識別子を含む上記暗号鍵管理リストを上記暗号鍵管理リストテーブルから検索して対応する上記ユニキャスト暗号鍵により上記ユニキャストフレームのペイロードを暗号化する手段と、暗号化された上記フレームを送信する手段とを具備する。これにより、送信するフレームの終点端末識別子に応じてブロードキャスト暗号鍵およびユニキャスト暗号鍵を使い分けることを可能にするという作用をもたらす。

また、本発明の請求項 8 記載の端末は、送信先端末のユニキャスト暗号鍵により自端末の端末識別子およびブロードキャスト暗号鍵を暗号化する手段と、上記暗号化された自端末の端末識別子およびブロードキャスト暗号鍵を上記送信先端末に送信する手段とを具備する。これにより、自端末のブロードキャスト暗号鍵を自端末の管理の下で配布するという作用をもたらす。

また、本発明の請求項 9 記載の端末は、他の端末の端末識別子に対応して上記他の端末のブロードキャスト暗号鍵を保持する暗号鍵管理リストを少なくとも一つ有する暗号鍵管理リストテーブルと、送信先端末のユニキャスト暗号鍵により上記暗号鍵管理リストを暗号化する手段と、上記暗号化された暗号鍵管理リストを上記送信先端末に送信する手段とを具備する。これにより、自端末の管理するブロードキャスト暗号鍵群（暗号鍵管理リスト）を自律分散して配布するという作用をもたらす。

また、本発明の請求項 10 記載の端末は、他の端末から当該他の端末の端末識別子およびブロードキャスト暗号鍵を受信する手段と、自端末



のブロードキャスト暗号鍵により上記他の端末の端末識別子およびブロードキャスト暗号鍵を暗号化する手段と、上記暗号化された他の端末の端末識別子およびブロードキャスト暗号鍵をブロードキャスト配布する手段とを具備する。これにより、他の端末のブロードキャスト暗号鍵を  
5 自律分散して配布するという作用をもたらす。

また、本発明の請求項 1 1 記載のブロードキャストフレームの復号方法は、他の端末の端末識別子と上記他の端末のブロードキャスト暗号鍵との組からなる暗号鍵管理リストを少なくとも一つ有する暗号鍵管理リストテーブルを備える端末におけるブロードキャストフレームの復号方法  
10 法であって、受信したブロードキャストフレームの始点端末識別子を含む上記暗号鍵管理リストを上記暗号鍵管理リストテーブルから検索して対応する上記ブロードキャスト暗号鍵を抽出する手順と、抽出された上記ブロードキャスト暗号鍵により上記ブロードキャストフレームのペイロードを復号する手順とを具備する。これにより、ブロードキャストフ  
15 レームの始点端末識別子に応じて復号化に使用するブロードキャスト暗号鍵を選択可能にするという作用をもたらす。

また、本発明の請求項 1 2 記載のブロードキャストフレームの暗号化方法は、自端末のブロードキャスト暗号鍵を保持する生成鍵テーブルを備える端末におけるブロードキャストフレームの暗号化方法であって、  
20 ブロードキャストフレームのペイロードを上記生成鍵テーブルに保持されたブロードキャスト暗号鍵により暗号化する手順と、暗号化された上記ブロードキャストフレームを送信する手順とを具備する。これにより、ブロードキャスト通信を行う際に端末毎に異なるブロードキャスト暗号鍵によりブロードキャストフレームを暗号化することを可能にするとい  
25 う作用をもたらす。

また、本発明の請求項 1 3 記載のブロードキャスト暗号鍵配布方法は、

第1の端末と第2の端末との間のユニキャスト暗号鍵により暗号化された第1の端末の端末識別子およびブロードキャスト暗号鍵を受信する手順と、上記暗号化された第1の端末の端末識別子およびブロードキャスト暗号鍵を上記ユニキャスト暗号鍵により復号する手順と、第2の端末の端末識別子およびブロードキャスト暗号鍵を上記ユニキャスト暗号鍵により暗号化する手順と、上記暗号化された第2の端末の端末識別子およびブロードキャスト暗号鍵を上記第1の端末に送信する手順とを具備する。これにより、第1の端末と第2の端末との間で互いのブロードキャスト暗号鍵を配布するという作用をもたらす。

また、本発明の請求項14記載のブロードキャスト暗号鍵配布方法は、第1の端末と第2の端末との間のユニキャスト暗号鍵により暗号化された第1の端末の端末識別子およびブロードキャスト暗号鍵を受信する手順と、上記暗号化された第1の端末の端末識別子およびブロードキャスト暗号鍵を上記ユニキャスト暗号鍵により復号する手順と、上記第1の端末の端末識別子およびブロードキャスト暗号鍵を第2の端末のブロードキャスト暗号鍵により暗号化する手順と、上記暗号化された第1の端末の端末識別子およびブロードキャスト暗号鍵を第3の端末に送信する手順とを具備する。これにより、第1の端末のブロードキャスト暗号鍵を第3の端末にブロードキャスト配布するという作用をもたらす。

また、本発明の請求項15記載のプログラムは、他の端末の端末識別子と上記他の端末のブロードキャスト暗号鍵との組からなる暗号鍵管理リストを少なくとも一つ有する暗号鍵管理リストテーブルを備える端末において、受信したブロードキャストフレームの始点端末識別子を含む上記暗号鍵管理リストを上記暗号鍵管理リストテーブルから検索して対応する上記ブロードキャスト暗号鍵を抽出する手順と、抽出された上記ブロードキャスト暗号鍵により上記ブロードキャストフレームのペイロ

ードを復号する手順とを端末に実行させるものである。これにより、ブロードキャストフレームの始点端末識別子に応じて復号化に使用するブロードキャスト暗号鍵を選択可能にするという作用をもたらす。

また、本発明の請求項 16 記載のプログラムは、自端末のブロードキャスト暗号鍵を保持する生成鍵テーブルを備える端末において、ブロードキャストフレームのペイロードを上記生成鍵テーブルに保持されたブロードキャスト暗号鍵により暗号化する手順と、暗号化された上記ブロードキャストフレームを送信する手順とを端末に実行させるものである。これにより、ブロードキャスト通信を行う際に端末毎に異なるブロードキャスト暗号鍵によりブロードキャストフレームを暗号化することを可能にするという作用をもたらす。

また、本発明の請求項 17 記載のプログラムは、第 1 の端末と第 2 の端末との間のユニキャスト暗号鍵により暗号化された第 1 の端末の端末識別子およびブロードキャスト暗号鍵を受信する手順と、上記暗号化された第 1 の端末の端末識別子およびブロードキャスト暗号鍵を上記ユニキャスト暗号鍵により復号する手順と、第 2 の端末の端末識別子およびブロードキャスト暗号鍵を上記ユニキャスト暗号鍵により暗号化する手順と、上記暗号化された第 2 の端末の端末識別子およびブロードキャスト暗号鍵を上記第 1 の端末に送信する手順とを上記第 2 の端末に実行させるものである。これにより、第 1 の端末と第 2 の端末との間で互いのブロードキャスト暗号鍵を配布するという作用をもたらす。

また、本発明の請求項 18 記載のプログラムは、第 1 の端末と第 2 の端末との間のユニキャスト暗号鍵により暗号化された第 1 の端末の端末識別子およびブロードキャスト暗号鍵を受信する手順と、上記暗号化された第 1 の端末の端末識別子およびブロードキャスト暗号鍵を上記ユニキャスト暗号鍵により復号する手順と、上記第 1 の端末の端末識別子お

よびブロードキャスト暗号鍵を第 2 の端末のブロードキャスト暗号鍵により暗号化する手順と、上記暗号化された第 1 の端末の端末識別子およびブロードキャスト暗号鍵を第 3 の端末に送信する手順とを上記第 2 の  
5 端末に実行させるものである。これにより、第 1 の端末のブロードキャスト暗号鍵を第 3 の端末にブロードキャスト配布するという作用をもたらす。

#### 図面の簡単な説明

図 1 は、本発明の実施の形態における無線アドホック通信システムにおいて使用される無線端末 3 0 0 の構成例を示す図である。

図 2 は、本発明の実施の形態における属性証明書発行端末リストテーブル 6 1 0 の構成例を示す図である。

図 3 は、本発明の実施の形態における属性証明書発行端末リストテーブル 6 1 0 に保持される公開鍵証明書 6 1 2 のフォーマット 7 1 0 を示す図である。

図 4 は、本発明の実施の形態における属性証明書テーブル 6 2 0 に保持される属性証明書のフォーマット 7 2 0 を示す図である。

図 5 は、本発明の実施の形態における暗号鍵管理リストテーブル 6 6 0 の構成例を示す図である。

図 6 A および図 6 B は、本発明の実施の形態におけるブロードキャスト暗号鍵およびユニキャスト暗号鍵の機能を示す図である。

図 7 は、本発明の実施の形態における経路テーブル 6 8 0 の構成例を示す図である。

図 8 は、本発明の実施の形態におけるブロードキャスト通信およびユニキャスト通信に用いられるフレーム構成を示す図である。

図 9 は、本発明の実施の形態における相互認証の手順を示す図である。

図 1 0 は、本発明の実施の形態におけるビーコンフレーム 8 1 0 の構成例を示す図である。

図 1 1 は、本発明の実施の形態における認証要求フレーム 8 7 0 の構成例を示す図である。

5 図 1 2 は、本発明の実施の形態における認証応答フレーム 8 8 0 の構成例を示す図である。

図 1 3 は、本発明の実施の形態における暗号鍵配布の手順を示す図である。

10 図 1 4 は、本発明の実施の形態におけるセッション鍵配布フレーム 8 2 0 の構成例を示す図である。

図 1 5 は、本発明の実施の形態におけるブロードキャスト鍵配布フレーム 8 3 0 の構成例を示す図である。

図 1 6 は、本発明の実施の形態におけるフレーム送信の際の暗号鍵選択アルゴリズムを示す図である。

15 図 1 7 は、本発明の実施の形態におけるフレーム送信の際の暗号鍵選択アルゴリズムを示す図である。

発明を実施するための最良の形態

次に本発明の実施の形態について図面を参照して詳細に説明する。

20 図 1 は、本発明の実施の形態における無線アドホック通信システムにおいて使用される無線端末 3 0 0 の構成例を示す図である。無線端末 3 0 0 は、通信処理部 3 2 0 と、制御部 3 3 0 と、表示部 3 4 0 と、操作部 3 5 0 と、スピーカ 3 6 0 と、マイク 3 7 0 と、メモリ 6 0 0 とを備え、これらの間をバス 3 8 0 が接続する構成となっている。また、通信  
25 処理部 3 2 0 にはアンテナ 3 1 0 が接続されている。通信処理部 3 2 0 は、アンテナ 3 1 0 を介して受信した信号からネットワークインターフ

エース層（データリンク層）のフレームを構成する。また、通信処理部 320 は、ネットワークインターフェース層のフレームをアンテナ 310 を介して送信する。

制御部 330 は、無線端末 300 全体を制御する。例えば、通信処理部 320 により構成されたフレームを参照して所定の処理を行う。また、制御部 330 は、タイマ 335 を有し、所定のイベントからの経過時間を計時する。表示部 340 は、所定の情報を表示するものであり、例えば、液晶ディスプレイ等が用いられ得る。操作部 350 は、無線端末 300 に対して外部から操作指示を行うためのものであり、例えば、キーボードやボタンスイッチ等が用いられ得る。スピーカ 360 は、音声を出力するものであり、無線端末 300 の利用者に対して注意を喚起したり他の端末と音声情報のやりとりを行うために用いられる。マイク 370 は、無線端末 300 に対して外部から音声入力を行うものであり、他の端末と音声情報のやりとりを行ったり操作指示を行うために用いられる。

メモリ 600 は、属性証明書の発行端末に関する情報を保持する属性証明書発行端末リストテーブル 610 と、無線端末 300 自身のアクセス権限を示す属性証明書を保持する属性証明書テーブル 620 と、無線端末 300 自身の生成鍵に関する情報として自端末の公開鍵と秘密鍵と公開鍵証明書とブロードキャスト暗号鍵とを保持する生成鍵テーブル 650 と、他の端末との間のユニキャスト暗号鍵および他の端末のブロードキャスト暗号鍵を保持する暗号鍵管理リストテーブル 660 とを格納する。

図 2 は、本発明の実施の形態における属性証明書発行端末リストテーブル 610 の構成例である。この属性証明書発行端末リストテーブル 610 は、過去に属性証明書を発行した実績のある端末に関する情報を保

持するものであり、属性証明書発行端末の端末識別子 6 1 1 のそれぞれ  
に対応して、公開鍵証明書 6 1 2 を保持している。端末識別子 6 1 1 は、  
ネットワーク内において端末を一意に識別するものであればよく、例え  
ば、イーサネット（登録商標）における MAC（Media Access  
5      s s      C o n t r o l）アドレス等を用いることができる。公開鍵証明  
書 6 1 2 は、対応する端末識別子 6 1 1 により識別される端末の公開鍵  
証明書である。公開鍵証明書とは、証明書所有者（サブジェクト）の本  
人性を証明するものであり、証明書所有者の公開鍵を含む。この公開鍵  
証明書は証明書発行者たる認証局（CA：Certificate A  
10    u t h o r i t y）によって署名される。

図 3 は、属性証明書発行端末リストテーブル 6 1 0 に保持される公開  
鍵証明書 6 1 2 のフォーマット 7 1 0 を示す図である。この公開鍵証明  
書のフォーマット 7 1 0 は、大きく分けて、署名前証明書 7 1 1 と、署  
名アルゴリズム 7 1 8 と、署名 7 1 9 とから構成される。署名前証明書  
15    7 1 1 は、シリアル番号 7 1 2 と、発行者 7 1 4 と、有効期限 7 1 5 と、  
所有者 7 1 6 と、所有者 7 1 6 と、所有者公開鍵 7 1 7 とを含む。

シリアル番号 7 1 2 は、公開鍵証明書のシリアル番号であり、認証局  
によって採番される。発行者 7 1 4 は、公開鍵証明書の発行者たる認証  
局の名前である。この発行者 7 1 4 とシリアル番号 7 1 2 とにより公開  
20    鍵証明書は一意に識別される。有効期限 7 1 5 は、公開鍵証明書の有効  
期限である。所有者 7 1 6 は、公開鍵証明書の所有者の名前である。所  
有者公開鍵 7 1 7 は、所有者 7 1 6 の公開鍵である。

署名 7 1 9 は公開鍵証明書に対する認証局による署名であり、署名ア  
ルゴリズム 7 1 8 はこの署名 7 1 9 のために使用された署名アルゴリズム  
25    ムである。署名アルゴリズムは、メッセージダイジェストアルゴリズム  
と公開鍵暗号アルゴリズムの 2 つにより構成される。メッセージダイジ

エストアルゴリズムは、ハッシュ関数（要約関数）の一つであり、署名前証明書 7 1 1 のメッセージダイジェストを作成するためのアルゴリズムである。ここで、メッセージダイジェストとは、入力データ（署名前証明書 7 1 1）を固定長のビット列に圧縮したものであり、拇印や指紋（フィンガープリント）等とも呼ばれる。メッセージダイジェストアルゴリズムとしては、SHA-1（Secure Hash Algorithm 1）、MD2（Message Digest #2）、MD5（Message Digest #5）等が知られている。公開鍵暗号アルゴリズムは、メッセージダイジェストアルゴリズムにより得られたメッセージダイジェストを認証局の秘密鍵により暗号化するためのアルゴリズムである。この公開鍵暗号アルゴリズムとしては、素因数分解問題に基づくRSAや離散対数問題に基づくDSA等が知られている。このように、署名前証明書 7 1 1 のメッセージダイジェストを認証局の秘密鍵により暗号化したものが署名 7 1 9 となる。

従って、この公開鍵証明書の署名 7 1 9 を認証局の公開鍵により復号することによってメッセージダイジェストが得られる。公開鍵証明書の利用者は、署名前証明書 7 1 1 のメッセージダイジェストを自身で作成し、それを認証局の公開鍵により復号されたメッセージダイジェストと比較することにより、署名前証明書 7 1 1 の内容が改ざんされていないことを検証できる。

図 4 は、属性証明書テーブル 6 2 0 に保持される属性証明書のフォーマット 7 2 0 を示す図である。この属性証明書は、大きく分けて、属性証明情報 7 2 1 と、署名アルゴリズム 7 2 8 と、署名 7 2 9 とから構成される。属性証明情報 7 2 1 は、所有者公開鍵証明書識別子 7 2 3 と、発行者 7 2 4 と、シリアル番号 7 2 2 と、有効期限 7 2 5 とを含む。

所有者公開鍵証明書識別子 7 2 3 は、属性証明書の所有者の公開鍵証



明書を識別するためのものである。具体的には、公開鍵証明書 7 1 0 (図 3) の発行者 7 1 4 とシリアル番号 7 1 2 とにより識別する。発行者 7 2 4 は、属性証明書の発行者たる属性認証局 (A A : A t t r i b u t e c e r t i f i c a t e A u t h o r i t y) の名称である。シ

5 リアル番号 7 2 2 は、属性証明書のシリアル番号であり、属性証明書の発行者たる属性認証局によって採番される。このシリアル番号 7 2 2 と発行者 7 2 4 とにより属性証明書は一意に識別される。有効期限 7 2 5 は、属性証明書の有効期限である。

署名 7 2 9 は属性証明書に対する属性認証局による署名であり、署名

10 アルゴリズム 7 2 8 はこの署名 7 2 9 のために使用された署名アルゴリズムである。署名アルゴリズムの内容については、前述の公開鍵証明書の署名アルゴリズム 7 1 8 と同様であり、属性証明情報 7 2 1 のメッセージダイジェストを属性認証局の秘密鍵により暗号化したものが署名 7 2 9 となる。

15 従って、この属性証明書の署名 7 2 9 を属性認証局の公開鍵により復号することによってメッセージダイジェストが得られる。属性証明書の利用者は、属性証明情報 7 2 1 のメッセージダイジェストを自身で作成し、それを属性認証局の公開鍵により復号されたメッセージダイジェストと比較することにより、属性証明情報 7 2 1 の内容が改ざんされていないことを検証できる。

20

なお、本明細書では、端末権限認証証明書の一例として属性証明書について説明するが、例えば、XML 言語等により端末権限を記述しておき、権限を有する機関がそれに署名を付することにより作成されたようなものであっても本発明における端末権限認証証明書として機能し得る。

25 図 5 は、本発明の実施の形態における暗号鍵管理リストテーブル 6 6 0 の構成例である。この暗号鍵管理リストテーブル 6 6 0 は、復号化に

用いられるブロードキャスト鍵および暗号化ならびに復号化に用いられるユニキャスト鍵を保持するものであり、他の端末の端末識別子 6 6 1 に対応して当該他の端末との間のユニキャスト暗号鍵 6 6 2 および当該他の端末のブロードキャスト暗号鍵 6 6 3 を保持する暗号鍵管理リスト

5 を少なくとも一つ有する。

端末識別子 6 6 1 は、上述の通り他の端末を一意に識別するものであり、一例として MAC アドレス等を用いることができる。ユニキャスト暗号鍵 6 6 2 は、対応する端末識別子 6 6 1 を有する端末との間のユニキャスト通信のために定められた共通鍵である。このユニキャスト暗号

10 鍵 6 6 2 を表すために、例えば、端末 A と端末 B との間で使用されるユニキャスト暗号鍵を「UK\_\_AB」等と表記する。また、ブロードキャスト暗号鍵 6 6 3 は、対応する端末識別子 6 6 1 を有する端末がブロードキャスト通信を行うために定められた共通鍵である。このブロードキャスト暗号鍵 6 6 3 を表すために、例えば、端末 B からのブロードキャスト通信において使用されるブロードキャスト暗号鍵を「BK\_\_B」等

15 と表記する。

なお、これらユニキャスト暗号鍵およびブロードキャスト暗号鍵に用いられる共通鍵アルゴリズムとしては、56 ビットの鍵の長さを有する DES (Data Encryption Standard)、12

20 8 ビット、192 ビットおよび 256 ビットの 3 通りの鍵の長さを有する AES (Advanced Encryption Standard) 等が知られている。

図 6 A および図 6 B は、本発明の実施の形態におけるブロードキャスト暗号鍵およびユニキャスト暗号鍵の機能を示す図である。ブロードキャスト暗号鍵は、ブロードキャスト通信を行う各端末毎に定められるものであり、ブロードキャスト送信端末における暗号化およびブロードキ

25

キャスト受信端末における復号化の両方で共通に用いられる共通鍵である。例えば、端末Aのブロードキャスト暗号鍵（BK\_\_A）は、端末Aがブロードキャスト通信を送信する際の暗号化に使用され、端末A以外の端末が端末Aからのブロードキャスト通信を受信する際の復号化に使用される。

一方、ユニキャスト暗号鍵は、端末対毎に定められるものであり、端末対における通信の暗号化および復号化の両方で共通に用いられる共通鍵である。例えば、端末Aと端末Bの間のユニキャスト暗号鍵（UK\_\_AB）は、端末Aが端末Bにユニキャスト通信を送信する際の暗号化および端末Bが端末Aからのユニキャスト通信を受信する際の復号化に使用されるだけでなく、端末Bが端末Aにユニキャスト通信を送信する際の暗号化および端末Aが端末Bからのユニキャスト通信を受信する際の復号化にも使用される。

図7は、本発明の実施の形態における経路テーブル680の構成例である。この経路テーブル680は、終点端末にフレームを到達させるための転送先端末に関する情報を保持するものであり、終点端末の端末識別子681に対応してフレームの転送先端末の端末識別子682および有効時間683を保持する経路リストを少なくとも一つ有する。

終点端末識別子681および転送先端末識別子682における端末識別子は、上述の通り他の端末を一意に識別するものである。ある端末に最終的にフレームを配送するために、次にどの端末にフレームを転送すべきであるかを示している。

無線アドホック通信システムにおいては、ネットワーク構成が時々刻々と変化する可能性がある。従って、経路テーブル680に保持される情報も古くなる可能性がある。そこで、有効時間683によって、対応する情報の鮮度を管理する。例えば、情報更新時もしくは情報更新から

の経過時間を有効時間 6 8 3 に記録していくことにより、所定時間以上経過した情報を削除もしくは更新することが考えられる。これらの時間を計時するために制御部 3 3 0 のタイマ 3 3 5 が使用される。

図 8 は、本発明の実施の形態におけるブロードキャスト通信およびユニキャスト通信に用いられるフレーム構成を示す図である。フレーム 8 0 0 は、ヘッダ部 8 0 1 と、ペイロード部 8 0 2 とから構成される。また、ヘッダ部 8 0 1 は、始点端末識別子 8 0 3 と、終点端末識別子 8 0 4 と、送信端末識別子 8 0 5 と、受信端末識別子 8 0 6 と、フレーム種別 8 0 7 と、属性証明書の有無 8 0 8 とを含む。始点端末識別子 8 0 3 は、このフレームを最初に発信した端末の端末識別子である。なお、端末識別子は、前述のようにネットワーク内において端末を一意に識別するものであればよく、例えば、イーサネット（登録商標）における MAC アドレス等を用いることができる。終点端末識別子 8 0 4 は、このフレームの最終宛先の端末の端末識別子である。

送信端末識別子 8 0 5 および受信端末識別子 8 0 6 は、フレームを中継する際に用いられる。無線アドホック通信システムにおいては、ネットワーク内の全ての端末が直接通信できるとは限らず、電波の届かない端末へフレームを送信したい場合には他の端末を介してマルチホップにより通信経路を確立しなければならない。この場合にフレームの送受信を行う端末間で使用されるのが送信端末識別子 8 0 5 および受信端末識別子 8 0 6 である。フレーム種別 8 0 7 は、フレームの種別を示すものである。

ペイロード部 8 0 2 には通信の内容であるデータ 8 0 9 が格納される。このペイロード部 8 0 2 が、ユニキャスト暗号鍵およびブロードキャスト暗号鍵による暗号化および復号化の対象となる。

次に本発明の実施の形態における無線アドホック通信システムの動作

について図面を参照して説明する。本発明の実施の形態では、端末がネットワーク資源に接続する際に端末間で属性証明書を用いて相互認証（図 9）を行い、互いの認証に成功した後にセッション鍵の配布、ユニキャスト暗号鍵の生成、および、ブロードキャスト暗号鍵の配布を行う（図 13）。これら図 9 および図 13 における各処理は、無線端末 300 における制御部 330 により実現される。

なお、相互認証に用いられる属性証明書は、予め適切に発行されて、各端末の属性証明書テーブル 620（図 1）に保持されていることを前提とする。また、属性証明書の検証に必要な属性証明書発行端末の公開鍵は、各端末の属性証明書発行端末リストテーブル 610 の公開鍵証明書 612（図 2）に予め設定されていることを前提とする。

図 9 は、本発明の実施の形態における相互認証の手順を示す図である。本発明の実施の形態における無線アドホック通信システムでは、各端末は定期的にビーコンを送信し、他の端末に対して自己の存在を知らせる。以下では、端末 B のビーコンをトリガーとして端末 A が認証要求を行うものと仮定するが、最終的に相互に認証が行われればよく、何れの端末のビーコンをトリガーとしてもよい。

まず、端末 B が、ビーコン 2111 を送信しているものとする（211）。このビーコン 2111 のフレーム構成は図 10 の通りである。ビーコンフレーム 810 は、図 8 で説明したフレーム 800 の構成に基づくものであり、ヘッダ部 811 およびペイロード部 812 に分けられる点も同様である。各端末識別子 813 乃至 816 も図 8 の各端末識別子 803 乃至 806 と同様である。ビーコンフレーム 810 では、終点端末識別子 814 にはブロードキャストアドレス（例えば、全てのビットに 1）が設定される。フレーム種別 817 は、ここでは、ビーコンフレームであることを示す。属性証明書の有無 818 は、ネットワーク資源

にアクセスする権限を示す属性証明書をビーコンフレームの送信元端末が有しているか否かを示すものである。属性証明書を有していない旨をこの属性証明書の有無 8 1 8 が示している場合には、相互認証を進めることはできず、例えば、属性証明書の取得を促す等の処置を採ることが考えられる。

5 端末 A は、端末 B から送信されたビーコン 2 1 1 1 を受信すると (1 1 1)、ビーコンフレーム 8 1 0 の属性証明書の有無 8 1 8 をチェックする。端末 B が属性証明書を有していると判断すると、端末 A は端末 B に対して端末 A を認証するよう認証要求メッセージ 1 1 2 2 を送信する  
10 (1 1 2)。この認証要求メッセージ 1 1 2 2 のフレーム構成は図 1 1 の通りである。認証要求フレーム 8 7 0 は、図 8 で説明したフレーム 8 0 0 の構成に基づくものであり、ヘッダ部 8 7 1 およびペイロード部 8 7 2 に分けられる点も同様である。各端末識別子 8 7 3 乃至 8 7 6 も図 8 の各端末識別子 8 0 3 乃至 8 0 6 と同様である。フレーム種別 8 7 7  
15 は、ここでは、認証要求フレームであることを示す。

また、この認証要求フレーム 8 7 0 では、ペイロード部 8 7 2 のデータ 8 7 9 として、送信元である端末 A の公開鍵証明書 8 7 9 1 および属性証明書 8 7 9 2 が含まれる。端末 A の公開鍵証明書 8 7 9 1 は端末 A の生成鍵テーブル 6 5 0 に予め格納されたものであり、端末 A の属性証明書 8 7 9 2 は端末 A の属性証明書テーブル 6 2 0 に予め格納されたものである。

20 端末 B は、端末 A から送信された認証要求メッセージ 1 1 2 2 を受信すると、その内容から端末 A を認証する (2 1 2)。具体的には、属性証明書発行端末リストテーブル 6 1 0 の公開鍵証明書 6 1 2 (図 2) から属性認証局の公開鍵を抽出して、この公開鍵によって認証要求メッセージ 1 1 2 2 に含まれる属性証明書 8 7 9 2 の署名 7 2 9 (図 4) を復  
25

号することにより署名時のメッセージダイジェストを得る。そして、属性証明書 8 7 9 2 の属性証明情報 7 2 1 (図 4) のメッセージダイジェストを新たに生成する。この新たに生成されたメッセージダイジェストが署名時のメッセージダイジェストと一致していることを確認する。もしこれらが一致しないとすれば、属性証明書は署名後に改ざんされた可能性があり、属性証明書の検証は失敗となる。両者が一致している場合には、さらに認証要求メッセージ 1 1 2 2 に含まれる属性証明書 8 7 9 2 の所有者公開鍵証明書識別子 7 2 3 (図 4) が、認証要求メッセージ 1 1 2 2 に含まれる公開鍵証明書 8 7 9 1 の発行者 7 1 4 およびシリアル番号 7 1 2 (図 3) に一致することを確認する。これが一致すれば、公開鍵証明書の所有者である端末 A は属性証明書の所有者であることが確認できる。もしこれらが一致しなければ、属性証明書の所有者は端末 A ではなく、属性証明書の検証は失敗となる。

端末 A の認証 (2 1 2) に成功すると、端末 B は端末 A の認証に成功したことを通知する認証成功メッセージ 2 1 3 1 を端末 A に送信する (2 1 3)。この認証成功メッセージ 2 1 3 1 の認証応答フレーム構成は図 1 2 の通りである。認証応答フレーム 8 8 0 は、図 8 で説明したフレーム 8 0 0 の構成に基づくものであり、ヘッダ部 8 8 1 およびペイロード部 8 8 2 に分けられる点も同様である。各端末識別子 8 8 3 乃至 8 8 6 も図 8 の各端末識別子 8 0 3 乃至 8 0 6 と同様である。認証成功メッセージ 2 1 3 1 の場合、フレーム種別 8 8 7 は認証成功フレームとなる。この認証応答フレーム 8 8 0 では、さらに応答理由種別 8 8 8 を含むが、認証成功の場合は特に必要はない。

なお、端末 A の属性証明書の検証 (2 1 2) に失敗すると、端末 B は端末 A の認証に成功したことを通知する認証失敗メッセージを端末 A に送信することになる。この認証失敗メッセージの認証応答フレーム構成

は図 1 2 により説明した通りである。但し、認証失敗メッセージの場合、フレーム種別 8 8 7 は認証失敗フレームとなり、応答理由種別 8 8 8 には認証に失敗した理由として属性証明書のメッセージダイジェスト不一致、属性証明書失効等の事由がコード化されて示される。これら。認証  
5 成功メッセージ 2 1 3 1 または認証失敗メッセージは端末 A において受信されて確認される (1 1 3)。

端末 A の属性証明書の検証 (2 1 2) に成功すると、さらに端末 B は端末 A に対して端末 B を認証するよう認証要求メッセージ 2 1 4 1 を送信する (2 1 4)。この認証要求メッセージ 2 1 4 1 のフレーム構成は  
10 上述の図 1 1 と同様であり、送信元である端末 B の公開鍵証明書 8 7 9 1 および属性証明書 8 7 9 2 が含まれる。

端末 A は、端末 B から送信された認証要求メッセージ 2 1 4 1 を受信すると、その内容から端末 B を認証する (1 1 4)。この認証の内容は、既に説明した端末 B における端末 A の認証 (2 1 2) と同様であり、属  
15 性証明書の検証、および、属性証明書の所有者の確認等を行う。

端末 B の認証 (2 1 2) に成功すると、端末 A は端末 B の認証に成功したことを通知する認証成功メッセージ 1 1 5 2 を端末 B に送信する (1 1 5)。この認証成功メッセージ 1 1 5 2 の認証応答フレーム構成は上述の図 1 2 と同様である。また、端末 B の属性証明書の検証 (2 1  
20 2) に失敗した場合には、端末 A は端末 B の認証に成功したことを通知する認証失敗メッセージを端末 B に送信することになる。この認証失敗メッセージの認証応答フレーム構成も図 1 2 により説明した通りである。これら認証成功メッセージ 1 1 5 2 または認証失敗メッセージは端末 B において受信されて確認される (2 1 5)。

25 このようにして、端末 A および端末 B において互いの端末の認証に成功すると相互認証は完了し、次に暗号鍵の配布を行う。



図13は、本発明の実施の形態における暗号鍵配布の手順を示す図である。ここで、端末A(100)は新規にネットワークに参入しようとしている端末であり、端末B(200)は既にネットワークに参入している属性証明書発行端末である。

- 5      まず、端末Aは、端末Bとの間で通信を行うためのセッション鍵を生成する(121)。このセッション鍵は、端末Aと端末Bとの間の共通鍵であり、乱数を用いて生成することができる。端末Aは、このセッション鍵を端末Bの公開鍵により暗号化してセッション鍵配布メッセージ1222として端末Bに送信する(122)。このセッション鍵配布メ  
10      ヌッセージ1222のセッション鍵配布フレーム構成は図14の通りである。セッション鍵配布フレーム820は、図8で説明したフレーム800の構成に基づくものであり、ヘッダ部821およびペイロード部822に分けられる点も同様である。各端末識別子823乃至826も図8の各端末識別子803乃至806と同様である。フレーム種別827は  
15      セッション鍵配布フレームとなる。ペイロード部822のデータ829にはセッション鍵8291が含まれる。

- なお、このセッション鍵配布フレームのペイロード部822は、ユニキャスト暗号鍵またはブロードキャスト暗号鍵による暗号化または復号  
20      化の対象とはならず、受信端末の公開鍵で暗号化され、受信端末の秘密鍵で復号化される。端末Aは、相互認証の段階で端末Bの公開鍵証明書を  
        受信しているため、その所有者公開鍵717(図3)により端末Bの公開鍵を得ることができる。

- 端末Bは、端末Aから送信されたセッション鍵配布メッセージ1222を受信すると、セッション鍵8291を端末Bの秘密鍵により復号化  
25      する(222)。これにより、端末Aおよび端末Bの間で同一のセッション鍵を共有したことになる。

その後、端末Aおよび端末Bは、セッション鍵からユニキャスト暗号鍵（UK\_\_AB）を生成する（1 2 3、2 2 3）。このユニキャスト暗号鍵は、セッション鍵をそのまま利用してもよく、また、このセッション鍵を種（シード）としてハッシュ関数により新たにユニキャスト暗号鍵を生成するようにしてもよい。このようにして得られた端末Aと端末Bとの間のユニキャスト暗号鍵（UK\_\_AB）は、両端末の暗号鍵管理リストテーブル6 6 0の対応するユニキャスト暗号鍵6 6 2（図5）に格納される。

次に、端末Aは、予め生成していた端末Aのブロードキャスト暗号鍵（BK\_\_A）と端末Aの端末識別子との対を端末Bとの間のユニキャスト暗号鍵（UK\_\_AB）により暗号化してブロードキャスト鍵配布メッセージ1 2 4 2として端末Bに送信する（1 2 4）。このブロードキャスト鍵配布メッセージ1 2 4 2のブロードキャスト鍵配布フレーム構成は図1 5の通りである。ブロードキャスト鍵配布フレーム8 3 0は、図8で説明したフレーム8 0 0の構成に基づくものであり、ヘッダ部8 3 1およびペイロード部8 3 2に分けられる点も同様である。各端末識別子8 3 3乃至8 3 6も図8の各端末識別子8 0 3乃至8 0 6と同様である。フレーム種別8 3 7はブロードキャスト鍵配布フレームとなる。ペイロード部8 3 2のデータ8 3 9には端末識別子8 3 9 1とブロードキャスト暗号鍵8 3 9 2との対が含まれる。端末Aは、端末Aのブロードキャスト暗号鍵（BK\_\_A）8 3 9 2を生成鍵テーブル6 5 0に保持している。また、ブロードキャスト鍵配布メッセージ1 2 4 2のペイロード部8 3 2の暗号化に用いるユニキャスト暗号鍵（UK\_\_AB）は暗号鍵管理リストテーブル6 6 0のユニキャスト暗号鍵6 6 2（図5）に保持している。

端末Bは、端末Aからブロードキャスト鍵配布メッセージ1 2 4 2を

受信すると、ブロードキャスト鍵配布メッセージ 1 2 4 2 のペイロード部 8 3 2 を端末 A との間のユニキャスト暗号鍵 (UK\_\_AB) により復号化する (2 2 4)。これにより、端末 A のブロードキャスト暗号鍵と端末識別子とを取得する。そして、この端末 A のブロードキャスト暗号鍵を端末 A の端末識別子と関連付けて、暗号鍵管理リストテーブル 6 6 0 のブロードキャスト暗号鍵 6 6 3 (図 5) に格納する。

そして、端末 B は、端末 A のブロードキャスト暗号鍵 (BK\_\_A) と端末 A の端末識別子との対を端末 B のブロードキャスト暗号鍵 (BK\_\_B) により暗号化してブロードキャスト鍵配布メッセージ 2 2 4 4 として他の端末にブロードキャスト送信する (2 2 5)。このブロードキャスト鍵配布メッセージ 2 2 4 4 のブロードキャスト鍵配布フレーム構成は上述した図 1 5 の通りであるが、終点端末識別子 8 3 4 にはブロードキャストアドレス (例えば、全てのビットに 1) が設定される。

端末 B からのブロードキャスト鍵配布メッセージ 2 2 4 4 を受信した他の端末 4 0 0 (例えば、端末 C や端末 D) は、ブロードキャスト鍵配布メッセージ 2 2 4 4 のペイロード部 8 3 2 を端末 B のブロードキャスト暗号鍵 (BK\_\_B) により復号化する (4 2 5)。これにより、端末 A のブロードキャスト暗号鍵と端末識別子とを取得する。そして、この端末 A のブロードキャスト暗号鍵を端末 A の端末識別子と関連付けて、暗号鍵管理リストテーブル 6 6 0 のブロードキャスト暗号鍵 6 6 3 (図 5) に格納する。

さらに、端末 B は、端末 B の暗号鍵管理リストテーブル 6 6 0 に含まれるブロードキャスト暗号鍵 6 6 3 の全てをそれぞれの端末識別子 6 6 1 と対にして、端末 A との間のユニキャスト暗号鍵 (UK\_\_AB) により暗号化してブロードキャスト鍵配布メッセージ 2 2 6 1 として端末 A に送信する (2 2 6)。このブロードキャスト鍵配布メッセージ 2 2 6

1 のブロードキャスト鍵配布フレーム構成は上述した図 1 5 の通りであるが、ペイロード部 8 3 2 には端末識別子 8 3 9 1 およびブロードキャスト暗号鍵 8 3 9 2 の対が複数含まれる可能性がある。

5 端末 B からブロードキャスト鍵配布メッセージ 2 2 6 1 を受信した端末 A は、ブロードキャスト鍵配布メッセージ 2 2 6 1 のペイロード部 8 3 2 を端末 B との間のユニキャスト暗号鍵 (UK\_AB) により復号化する (1 2 6)。これにより、他の端末のブロードキャスト暗号鍵と端末識別子との対を取得する。そして、これら他の端末のブロードキャスト暗号鍵をそれぞれの端末の端末識別子と関連付けて、暗号鍵管理リスト  
10 テーブル 6 6 0 のブロードキャスト暗号鍵 6 6 3 (図 5) に格納する。

次に本発明の実施の形態における無線アドホック通信システムの各端末の暗号鍵選択アルゴリズムについて図面を参照して説明する。

図 1 6 は、本発明の実施の形態におけるフレーム送信の際の暗号鍵選択アルゴリズムを示す図である。図 8 のフレームにおいて、ブロードキャストフレームでは終点端末識別子 8 0 4 がブロードキャストアドレス  
15 であるので (ステップ S 9 2 1)、自端末のブロードキャスト暗号鍵によりペイロード部 8 0 2 を暗号化する (ステップ S 9 2 2)。一方、ブロードキャストフレームでなければ終点端末識別子 8 0 4 がブロードキャストアドレス以外であるので (ステップ S 9 2 1)、終点端末識別子  
20 8 0 4 と一致する端末識別子 6 6 1 に対応するユニキャスト暗号鍵 6 6 2 を図 5 の暗号鍵管理リストテーブル 6 6 0 から抽出して、そのユニキャスト暗号鍵によりペイロード部 8 0 2 を暗号化する (ステップ S 9 2 3)。その後、暗号化されたフレームは下位層に送出される (ステップ S 9 2 4)。

25 図 1 7 は、本発明の実施の形態におけるフレーム受信の際の暗号鍵選択アルゴリズムを示す図である。図 8 のフレームにおいて、終点端末識

別子 804 がブロードキャストアドレスであれば(ステップ S911)、始点端末識別子 803 と一致する端末識別子 661 に対応するブロードキャスト暗号鍵 663 を図 5 の暗号鍵管理リストテーブル 660 から抽出して、そのブロードキャスト暗号鍵によりペイロード部 802 を復号化する(ステップ S912)。

終点端末識別子 804 がブロードキャストアドレスでなく(ステップ S911)、自端末の端末識別子であれば(ステップ S913)、始点端末識別子 803 と一致する端末識別子 661 に対応するユニキャスト暗号鍵 662 を図 5 の暗号鍵管理リストテーブル 660 から抽出して、そのユニキャスト暗号鍵によりペイロード部 802 を復号化する(ステップ S914)。ステップ S912 またはステップ S914 において復号化されたフレームは上位層において処理される(ステップ S915)。

一方、終点端末識別子 804 がブロードキャストアドレスでなく(ステップ S911)、自端末の端末識別子でもなければ(ステップ S913)、そのフレームは次点の端末へ転送される(ステップ S916)。次点の端末は、フレーム 800 の終点端末識別子 804 (図 8) と一致する終点端末識別子 681 を経路テーブル 680 (図 7) から抽出して、対応する転送先端末識別子 682 を参照することにより知ることができる。

このように、本発明の実施の形態によれば、暗号鍵管理リストテーブル 660 において端末識別子 661 に関連付けてブロードキャスト暗号鍵 663 を保持しておくことにより、端末毎に異なるブロードキャスト暗号鍵を適用することができる。これらブロードキャスト暗号鍵は、ブロードキャスト通信を行う端末自身が生成して図 13 のシーケンス等を用いて配布するものである。従って、無線アドホック通信システムのようにブロードキャスト暗号鍵の一元管理が適さない環境において、プロ

ードキャスト暗号鍵の管理を各端末において自律分散して行うことができる。

- 5      なお、本発明の実施の形態は、ネットワークに属する全ての端末へ均等に配送するブロードキャストに関するものであるが、この「ブロードキャスト」の語句は厳格に解釈されるものではなく、「マルチキャスト」を含む広い概念として解釈されるべきものである。

また、ここでは本発明の実施の形態を例示したものであり、本発明はこれに限られず、本発明の要旨を逸脱しない範囲において種々の変形を施すことができる。

- 10      また、ここで説明した処理手順はこれら一連の手順を有する方法として捉えてもよく、これら一連の手順をコンピュータに実行させるためのプログラム乃至そのプログラムを記憶する記録媒体として捉えてもよい。

#### 産業上の利用可能性

- 15      以上の説明で明らかなように、本発明によると、無線アドホック通信システムにおいて、ブロードキャスト暗号鍵の管理を自律分散して行うことができるという効果が得られる。

## 請求の範囲

1. 複数の端末により構成される無線アドホック通信システムであって、  
ブロードキャストフレームのペイロードを暗号化して当該ブロードキャストフレームを送信する第1の端末と、  
5 前記ブロードキャストフレームを受信して当該ブロードキャストフレームのペイロードを復号する第2の端末とを具備し、  
前記第1の端末は前記第1の端末のブロードキャスト暗号鍵により前記ブロードキャストフレームのペイロードを暗号化し、  
10 前記第2の端末は前記第1の端末のブロードキャスト暗号鍵により前記ブロードキャストフレームのペイロードを復号することを特徴とする無線アドホック通信システム。
2. 前記第2の端末は、  
15 前記第1の端末の端末識別子と前記第1の端末のブロードキャスト暗号鍵との組からなる暗号鍵管理リストを少なくとも有する暗号鍵管理リストテーブルと、  
受信したブロードキャストフレームの始点端末識別子に含まれる前記第1の端末の端末識別子により前記暗号鍵管理リストテーブルを検索して対応する前記第1の端末のブロードキャスト暗号鍵を抽出する手段と、  
20 抽出された前記第1の端末のブロードキャスト暗号鍵により前記ブロードキャストフレームのペイロードを復号する手段とを備えることを特徴とする請求項1記載の無線アドホック通信システム。
- 25 3. 前記第1の端末は、  
前記第1の端末のブロードキャスト暗号鍵を保持する生成鍵テーブル

と、

ブロードキャストフレームのペイロードを前記生成鍵テーブルに保持された前記第1の端末のブロードキャスト暗号鍵により暗号化する手段と、

- 5 暗号化された前記ブロードキャストフレームを送信する手段とを備えることを特徴とする請求項1記載の無線アドホック通信システム。

4. 他の端末の端末識別子と前記他の端末のブロードキャスト暗号鍵との組からなる暗号鍵管理リストを少なくとも一つ有する暗号鍵管理リストテーブルと、

受信したブロードキャストフレームの始点端末識別子を含む前記暗号鍵管理リストを前記暗号鍵管理リストテーブルから検索して対応する前記ブロードキャスト暗号鍵を抽出する手段と、

- 15 抽出された前記ブロードキャスト暗号鍵により前記ブロードキャストフレームのペイロードを復号する手段とを具備することを特徴とする端末。

5. 他の端末の端末識別子に対応して前記他の端末との間のユニキャスト暗号鍵および前記他の端末のブロードキャスト暗号鍵を保持する暗号鍵管理リストを少なくとも一つ有する暗号鍵管理リストテーブルと、

- 20 受信したフレームの終点端末識別子がブロードキャストアドレスであれば当該フレームの始点端末識別子を含む前記暗号鍵管理リストを前記暗号鍵管理リストテーブルから検索して対応する前記ブロードキャスト暗号鍵を暗号鍵として抽出し、前記受信したフレームの終点端末識別子がブロードキャストアドレス以外であれば当該フレームの始点端末識別子を含む前記暗号鍵管理リストを前記暗号鍵管理リストテーブルから検



索して対応する前記ユニキャスト暗号鍵を前記暗号鍵として抽出する手段と、

抽出された前記暗号鍵により前記フレームのペイロードを復号する手段とを具備することを特徴とする端末。

5

6. 自端末のブロードキャスト暗号鍵を保持する生成鍵テーブルと、

ブロードキャストフレームのペイロードを前記ブロードキャスト暗号鍵により暗号化する手段と、

暗号化された前記ブロードキャストフレームを送信する手段とを具備

10 することを特徴とする端末。

7. 自端末のブロードキャスト暗号鍵を保持する生成鍵テーブルと、

他の端末の端末識別子に対応して前記他の端末との間のユニキャスト暗号鍵を保持する暗号鍵管理リストを少なくとも一つ有する暗号鍵管理  
15 リストテーブルと、

送信しようとするフレームがブロードキャストフレームであれば前記生成鍵テーブルの前記ブロードキャスト暗号鍵により前記ブロードキャストフレームのペイロードを暗号化し、送信しようとする前記フレームがユニキャストフレームであれば当該ユニキャストフレームの終点端末  
20 識別子を含む前記暗号鍵管理リストを前記暗号鍵管理リストテーブルから検索して対応する前記ユニキャスト暗号鍵により前記ユニキャストフレームのペイロードを暗号化する手段と、

暗号化された前記フレームを送信する手段とを具備することを特徴とする端末。

25

8. 送信先端末のユニキャスト暗号鍵により自端末の端末識別子および

ブロードキャスト暗号鍵を暗号化する手段と、

前記暗号化された自端末の端末識別子およびブロードキャスト暗号鍵を前記送信先端末に送信する手段とを具備することを特徴とする端末。

- 5     9. 他の端末の端末識別子に対応して前記他の端末のブロードキャスト暗号鍵を保持する暗号鍵管理リストを少なくとも一つ有する暗号鍵管理リストテーブルと、

送信先端末のユニキャスト暗号鍵により前記暗号鍵管理リストを暗号化する手段と、

- 10     前記暗号化された暗号鍵管理リストを前記送信先端末に送信する手段とを具備することを特徴とする端末。

10. 他の端末から当該他の端末の端末識別子およびブロードキャスト暗号鍵を受信する手段と、

- 15     自端末のブロードキャスト暗号鍵により前記他の端末の端末識別子およびブロードキャスト暗号鍵を暗号化する手段と、

前記暗号化された他の端末の端末識別子およびブロードキャスト暗号鍵をブロードキャスト配布する手段とを具備することを特徴とする端末。

- 20     11. 他の端末の端末識別子と前記他の端末のブロードキャスト暗号鍵との組からなる暗号鍵管理リストを少なくとも一つ有する暗号鍵管理リストテーブルを備える端末におけるブロードキャストフレームの復号方法であって、

- 25     受信したブロードキャストフレームの始点端末識別子を含む前記暗号鍵管理リストを前記暗号鍵管理リストテーブルから検索して対応する前記ブロードキャスト暗号鍵を抽出する手順と、

抽出された前記ブロードキャスト暗号鍵により前記ブロードキャストフレームのペイロードを復号する手順とを具備することを特徴とするブロードキャストフレームの復号方法。

- 5    1 2. 自端末のブロードキャスト暗号鍵を保持する生成鍵テーブルを備える端末におけるブロードキャストフレームの暗号化方法であって、

ブロードキャストフレームのペイロードを前記生成鍵テーブルに保持されたブロードキャスト暗号鍵により暗号化する手順と、

- 10    暗号化された前記ブロードキャストフレームを送信する手順とを具備することを特徴とするブロードキャストフレームの暗号化方法。

1 3. 第 1 の端末と第 2 の端末との間のユニキャスト暗号鍵により暗号化された第 1 の端末の端末識別子およびブロードキャスト暗号鍵を受信する手順と、

- 15    前記暗号化された第 1 の端末の端末識別子およびブロードキャスト暗号鍵を前記ユニキャスト暗号鍵により復号する手順と、

第 2 の端末の端末識別子およびブロードキャスト暗号鍵を前記ユニキャスト暗号鍵により暗号化する手順と、

- 20    前記暗号化された第 2 の端末の端末識別子およびブロードキャスト暗号鍵を前記第 1 の端末に送信する手順とを具備することを特徴とする前記第 2 の端末におけるブロードキャスト暗号鍵配布方法。

- 25    1 4. 第 1 の端末と第 2 の端末との間のユニキャスト暗号鍵により暗号化された第 1 の端末の端末識別子およびブロードキャスト暗号鍵を受信する手順と、

前記暗号化された第 1 の端末の端末識別子およびブロードキャスト暗

号鍵を前記ユニキャスト暗号鍵により復号する手順と、

前記第 1 の端末の端末識別子およびブロードキャスト暗号鍵を第 2 の端末のブロードキャスト暗号鍵により暗号化する手順と、

- 前記暗号化された第 1 の端末の端末識別子およびブロードキャスト暗号鍵を第 3 の端末に送信する手順とを具備することを特徴とする前記第 2 の端末におけるブロードキャスト暗号鍵配布方法。

- 15 1 5. 他の端末の端末識別子と前記他の端末のブロードキャスト暗号鍵との組からなる暗号鍵管理リストを少なくとも一つ有する暗号鍵管理リストテーブルを備える端末において、

受信したブロードキャストフレームの始点端末識別子を含む前記暗号鍵管理リストを前記暗号鍵管理リストテーブルから検索して対応する前記ブロードキャスト暗号鍵を抽出する手順と、

- 20 抽出された前記ブロードキャスト暗号鍵により前記ブロードキャストフレームのペイロードを復号する手順とを端末に実行させることを特徴とするプログラム。

1 6. 自端末のブロードキャスト暗号鍵を保持する生成鍵テーブルを備える端末において、

- 20 ブロードキャストフレームのペイロードを前記生成鍵テーブルに保持されたブロードキャスト暗号鍵により暗号化する手順と、

暗号化された前記ブロードキャストフレームを送信する手順とを端末に実行させることを特徴とするプログラム。

- 25 1 7. 第 1 の端末と第 2 の端末との間のユニキャスト暗号鍵により暗号化された第 1 の端末の端末識別子およびブロードキャスト暗号鍵を受信

する手順と、

前記暗号化された第1の端末の端末識別子およびブロードキャスト暗号鍵を前記ユニキャスト暗号鍵により復号する手順と、

- 第2の端末の端末識別子およびブロードキャスト暗号鍵を前記ユニキャスト暗号鍵により暗号化する手順と、
- 5

前記暗号化された第2の端末の端末識別子およびブロードキャスト暗号鍵を前記第1の端末に送信する手順とを前記第2の端末に実行させることを特徴とするプログラム。

- 10 18. 第1の端末と第2の端末との間のユニキャスト暗号鍵により暗号化された第1の端末の端末識別子およびブロードキャスト暗号鍵を受信する手順と、

前記暗号化された第1の端末の端末識別子およびブロードキャスト暗号鍵を前記ユニキャスト暗号鍵により復号する手順と、

- 15 前記第1の端末の端末識別子およびブロードキャスト暗号鍵を第2の端末のブロードキャスト暗号鍵により暗号化する手順と、

前記暗号化された第1の端末の端末識別子およびブロードキャスト暗号鍵を第3の端末に送信する手順とを前記第2の端末に実行させることを特徴とするプログラム。

## 補正書の請求の範囲

補正書の請求の範囲〔2004年7月16日（16.07.04）国際事務局受理：出願当初の請求の範囲1—12、14—16及び18は補正された；他の請求の範囲は変更なし。（7頁）〕

1. （補正後）複数の端末により構成される無線アドホック通信システムであって、

5   ブロードキャストフレームのペイロードを暗号化して当該ブロードキャストフレームを送信する第1の端末と、

前記ブロードキャストフレームを受信して当該ブロードキャストフレームのペイロードを復号する第2の端末とを具備し、

10   前記第1の端末は前記第1の端末に割当てられたブロードキャスト暗号鍵により前記ブロードキャストフレームのペイロードを暗号化し、  
前記第2の端末は前記第1の端末に割当てられたブロードキャスト暗号鍵により前記ブロードキャストフレームのペイロードを復号することを特徴とする無線アドホック通信システム。

15   2. （補正後）前記第2の端末は、

前記第1の端末の端末識別子と前記第1の端末に割当てられたブロードキャスト暗号鍵との組からなる暗号鍵管理リストを少なくとも有する暗号鍵管理リストテーブルと、

20   受信したブロードキャストフレームの始点端末識別子に含まれる前記第1の端末の端末識別子により前記暗号鍵管理リストテーブルを検索して対応する前記第1の端末に割当てられたブロードキャスト暗号鍵を抽出する手段と、

25   抽出された前記第1の端末に割当てられたブロードキャスト暗号鍵により前記ブロードキャストフレームのペイロードを復号する手段とを備えることを特徴とする請求項1記載の無線アドホック通信システム。

3. （補正後）前記第1の端末は、

前記第1の端末に割当てられたブロードキャスト暗号鍵を保持する生成鍵テーブル

と、

ブロードキャストフレームのペイロードを前記生成鍵テーブルに保持された前記第1の端末に割当てられたブロードキャスト暗号鍵により暗号化する手段と、

- 5 暗号化された前記ブロードキャストフレームを送信する手段とを備えることを特徴とする請求項1記載の無線アドホック通信システム。

4. (補正後) 他の端末の端末識別子と前記他の端末に割当てられたブロードキャスト暗号鍵との組からなる暗号鍵管理リストを少なくとも一つ有する暗号鍵管理リストテーブルと、

- 10 受信したブロードキャストフレームの始点端末識別子を含む前記暗号鍵管理リストを前記暗号鍵管理リストテーブルから検索して対応する前記ブロードキャスト暗号鍵を抽出する手段と、

抽出された前記ブロードキャスト暗号鍵により前記ブロードキャストフ

- 15 レームのペイロードを復号する手段とを具備することを特徴とする端末。

5. (補正後) 他の端末の端末識別子に対応して前記他の端末との間のユニキャスト暗号鍵および前記他の端末に割当てられたブロードキャスト暗号鍵を保持する暗号鍵管理リストを少なくとも一つ有する暗号鍵管理リストテーブルと、

- 20 受信したフレームの終点端末識別子がブロードキャストアドレスであれば当該フレームの始点端末識別子を含む前記暗号鍵管理リストを前記暗号鍵管理リストテーブルから検索して対応する前記ブロードキャスト暗号鍵を暗号鍵として抽出し、前記受信したフレームの終点端末識別子が  
25 ブロードキャストアドレス以外であれば当該フレームの始点端末識別子を含む前記暗号鍵管理リストを前記暗号鍵管理リストテーブルから検

索して対応する前記ユニキャスト暗号鍵を前記暗号鍵として抽出する手段と、

抽出された前記暗号鍵により前記フレームのペイロードを復号する手段とを具備することを特徴とする端末。

5

6. (補正後) 自端末に割当てられたブロードキャスト暗号鍵を保持する生成鍵テーブルと、

ブロードキャストフレームのペイロードを前記ブロードキャスト暗号鍵により暗号化する手段と、

10 暗号化された前記ブロードキャストフレームを送信する手段とを具備することを特徴とする端末。

7. (補正後) 自端末に割当てられたブロードキャスト暗号鍵を保持する生成鍵テーブルと、

15 他の端末の端末識別子に対応して前記他の端末との間のユニキャスト暗号鍵を保持する暗号鍵管理リストを少なくとも一つ有する暗号鍵管理リストテーブルと、

送信しようとするフレームがブロードキャストフレームであれば前記生成鍵テーブルの前記ブロードキャスト暗号鍵により前記ブロードキャストフレームのペイロードを暗号化し、送信しようとする前記フレームがユニキャストフレームであれば当該ユニキャストフレームの終点端末識別子を含む前記暗号鍵管理リストを前記暗号鍵管理リストテーブルから検索して対応する前記ユニキャスト暗号鍵により前記ユニキャストフレームのペイロードを暗号化する手段と、

20 暗号化された前記フレームを送信する手段とを具備することを特徴とする端末。

8. (補正後) 送信先端末に割当てられたユニキャスト暗号鍵により自端末の端末識別子および

30



ブロードキャスト暗号鍵を暗号化する手段と、  
前記暗号化された自端末の端末識別子およびブロードキャスト暗号鍵を  
前記送信先端末に送信する手段とを具備することを特徴とする端末。

- 5     9. (補正後) 他の端末の端末識別子に対応して前記他の端末のブロー  
      ドキャスト暗号鍵を保持する暗号鍵管理リストを少なくとも一つ有する  
      暗号鍵管理リストテーブルと、  
      送信先端末に割当てられたユニキャスト暗号鍵により前記暗号鍵管理リ  
      ストを暗号化する手段と、
- 10    前記暗号化された暗号鍵管理リストを前記送信先端末に送信する手段と  
      を具備することを特徴とする端末。
10. (補正後) 他の端末から当該他の端末の端末識別子およびブロー  
      ドキャスト暗号鍵を受信する手段と、
- 15    自端末に割当てられたブロードキャスト暗号鍵により前記他の端末の端  
      末識別子およびブロードキャスト暗号鍵を暗号化する手段と、  
      前記暗号化された他の端末の端末識別子およびブロードキャスト暗号鍵  
      をブロードキャスト配布する手段とを具備することを特徴とする端末。
- 20    11. (補正後) 他の端末の端末識別子と前記他の端末に割当てられた  
      ブロードキャスト暗号鍵との組からなる暗号鍵管理リストを少なくとも  
      一つ有する暗号鍵管理リストテーブルを備える端末におけるブロードキ  
      ャストフレームの復号方法であって、  
      受信したブロードキャストフレームの始点端末識別子を含む前記暗号鍵  
25    管理リストを前記暗号鍵管理リストテーブルから検索して対応する前記  
      ブロードキャスト暗号鍵を抽出する手順と、

抽出された前記ブロードキャスト暗号鍵により前記ブロードキャストフレームのペイロードを復号する手順とを具備することを特徴とするブロードキャストフレームの復号方法。

- 5    1 2. (補正後) 自端末に割当てられたブロードキャスト暗号鍵を保持する生成鍵テーブルを備える端末におけるブロードキャストフレームの暗号化方法であって、  
ブロードキャストフレームのペイロードを前記生成鍵テーブルに保持されたブロードキャスト暗号鍵により暗号化する手順と、  
10   暗号化された前記ブロードキャストフレームを送信する手順とを具備することを特徴とするブロードキャストフレームの暗号化方法。

- 1 3. 第1の端末と第2の端末との間のユニキャスト暗号鍵により暗号化された第1の端末の端末識別子およびブロードキャスト暗号鍵を受信  
15   する手順と、

前記暗号化された第1の端末の端末識別子およびブロードキャスト暗号鍵を前記ユニキャスト暗号鍵により復号する手順と、

第2の端末の端末識別子およびブロードキャスト暗号鍵を前記ユニキャスト暗号鍵により暗号化する手順と、

- 20   前記暗号化された第2の端末の端末識別子およびブロードキャスト暗号鍵を前記第1の端末に送信する手順とを具備することを特徴とする前記第2の端末におけるブロードキャスト暗号鍵配布方法。

- 1 4. (補正後) 第1の端末と第2の端末との間のユニキャスト暗号鍵  
25   により暗号化された第1の端末の端末識別子およびブロードキャスト暗号鍵を受信する手順と、  
前記暗号化された第1の端末の端末識別子およびブロードキャスト暗

号鍵を前記ユニキャスト暗号鍵により復号する手順と、  
前記第 1 の端末の端末識別子およびブロードキャスト暗号鍵を第 2 の端末に割当てられたブロードキャスト暗号鍵により暗号化する手順と、  
前記暗号化された第 1 の端末の端末識別子およびブロードキャスト暗号  
5 鍵を第 3 の端末に送信する手順とを具備することを特徴とする前記第 2 の端末におけるブロードキャスト暗号鍵配布方法。

1 5. (補正後) 他の端末の端末識別子と前記他の端末に割当てられたブロードキャスト暗号鍵との組からなる暗号鍵管理リストを少なくとも  
10 一つ有する暗号鍵管理リストテーブルを備える端末において、  
受信したブロードキャストフレームの始点端末識別子を含む前記暗号鍵管理リストを前記暗号鍵管理リストテーブルから検索して対応する前記ブロードキャスト暗号鍵を抽出する手順と、  
抽出された前記ブロードキャスト暗号鍵により前記ブロードキャストフ  
15 レームのペイロードを復号する手順とを端末に実行させることを特徴とするプログラム。

1 6. (補正後) 自端末に割当てられたブロードキャスト暗号鍵を保持する生成鍵テーブルを備える端末において、  
20 ブロードキャストフレームのペイロードを前記生成鍵テーブルに保持されたブロードキャスト暗号鍵により暗号化する手順と、  
暗号化された前記ブロードキャストフレームを送信する手順とを端末に実行させることを特徴とするプログラム。

25 1 7. 第 1 の端末と第 2 の端末との間のユニキャスト暗号鍵により暗号化された第 1 の端末の端末識別子およびブロードキャスト暗号鍵を受信

する手順と、

前記暗号化された第 1 の端末の端末識別子およびブロードキャスト暗号鍵を前記ユニキャスト暗号鍵により復号する手順と、

- 第 2 の端末の端末識別子およびブロードキャスト暗号鍵を前記ユニキャスト暗号鍵により暗号化する手順と、
- 5

前記暗号化された第 2 の端末の端末識別子およびブロードキャスト暗号鍵を前記第 1 の端末に送信する手順とを前記第 2 の端末に実行させることを特徴とするプログラム。

- 10 18. (補正後) 第 1 の端末と第 2 の端末との間のユニキャスト暗号鍵により暗号化された第 1 の端末の端末識別子およびブロードキャスト暗号鍵を受信する手順と、

前記暗号化された第 1 の端末の端末識別子およびブロードキャスト暗号鍵を前記ユニキャスト暗号鍵により復号する手順と、

- 15 前記第 1 の端末の端末識別子およびブロードキャスト暗号鍵を第 2 の端末に割当てられたブロードキャスト暗号鍵により暗号化する手順と、
- 前記暗号化された第 1 の端末の端末識別子およびブロードキャスト暗号鍵を第 3 の端末に送信する手順とを前記第 2 の端末に実行させることを特徴とするプログラム。

1/17

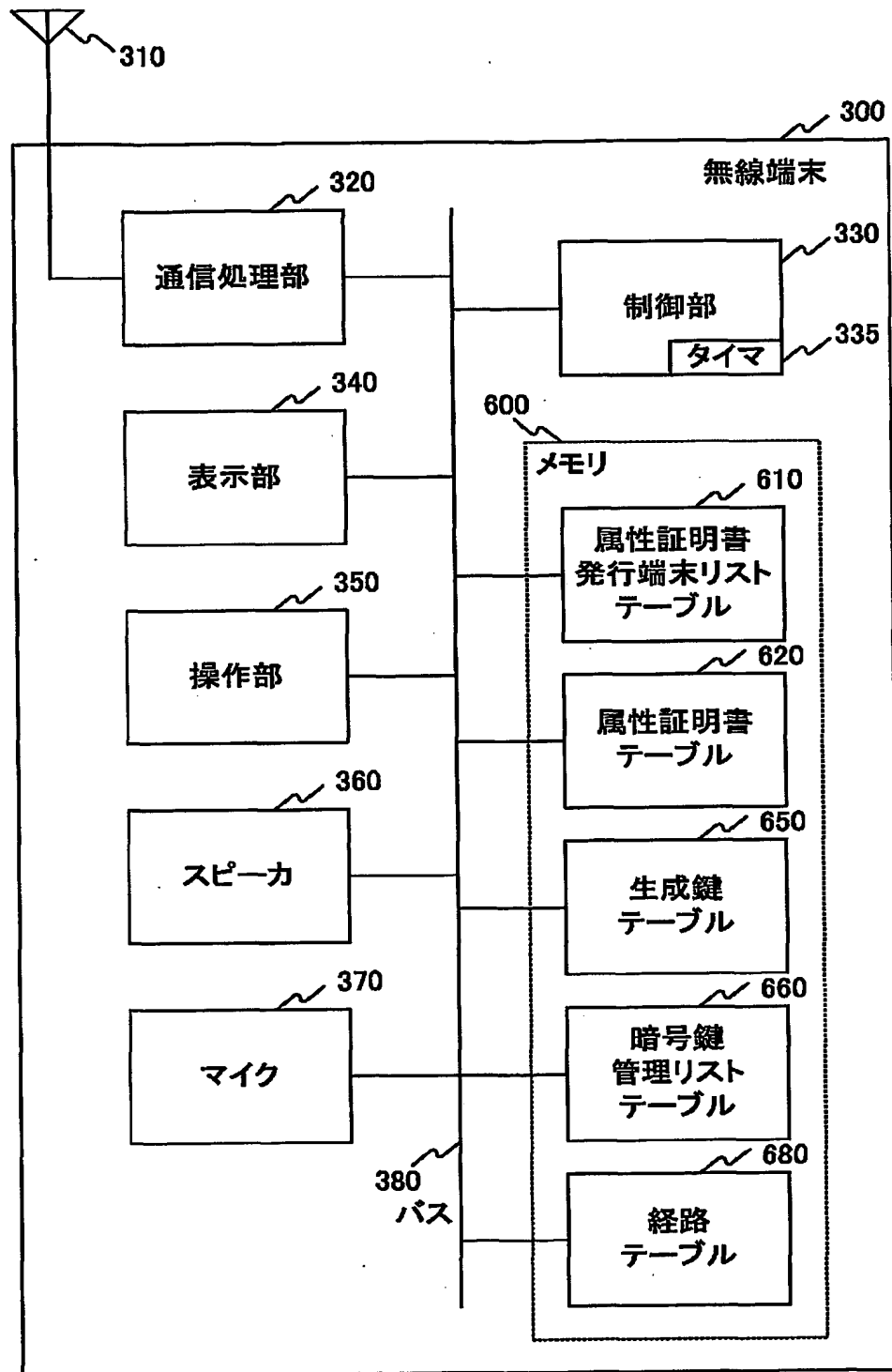


Fig.1

2/17

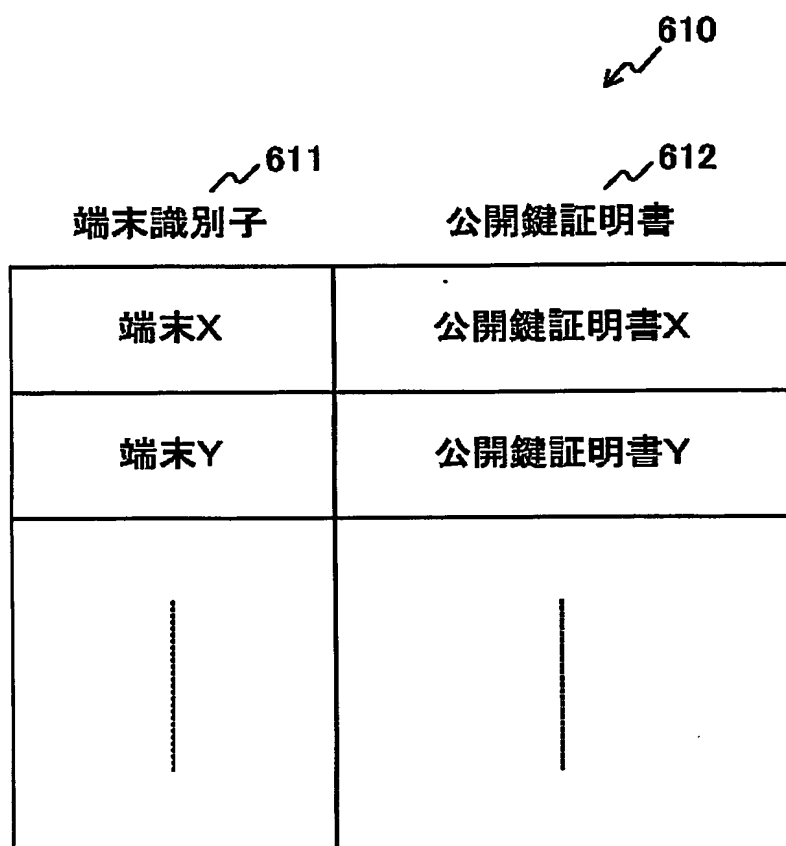


Fig.2

3/17

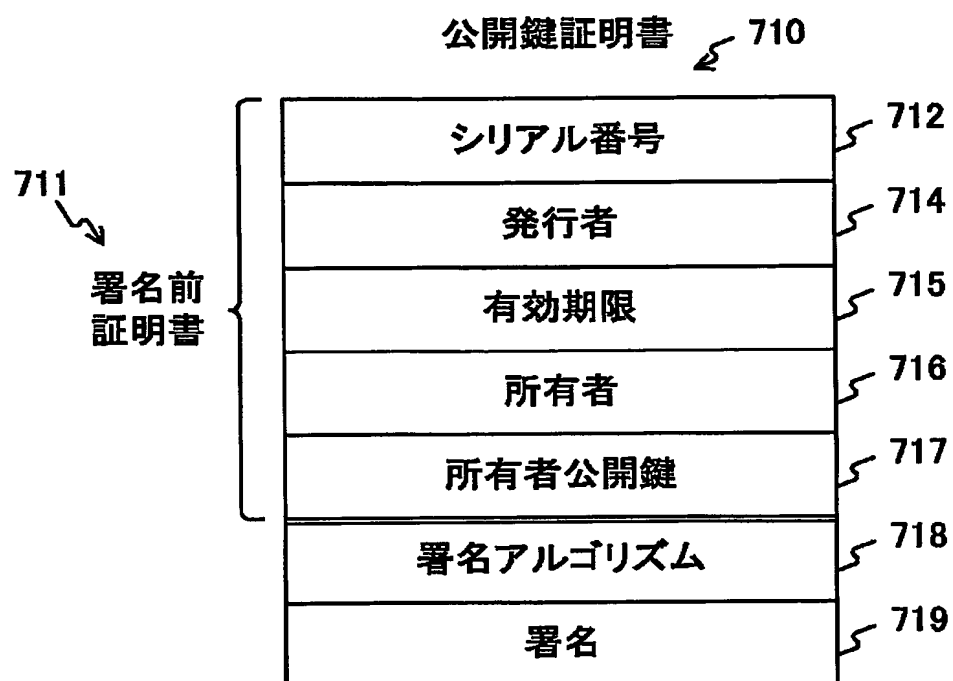


Fig.3

4/17

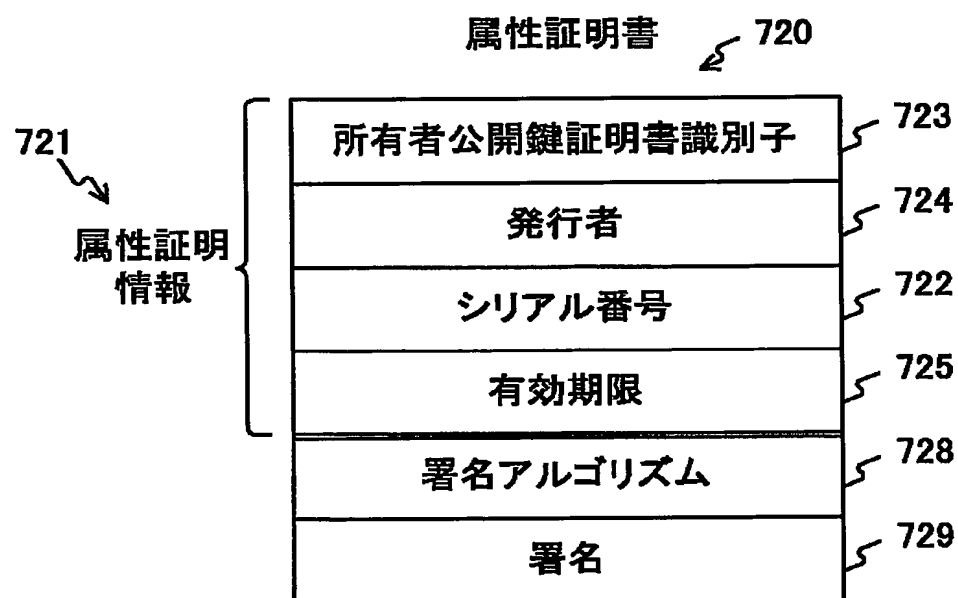


Fig.4



5/17

660

661                      662                      663

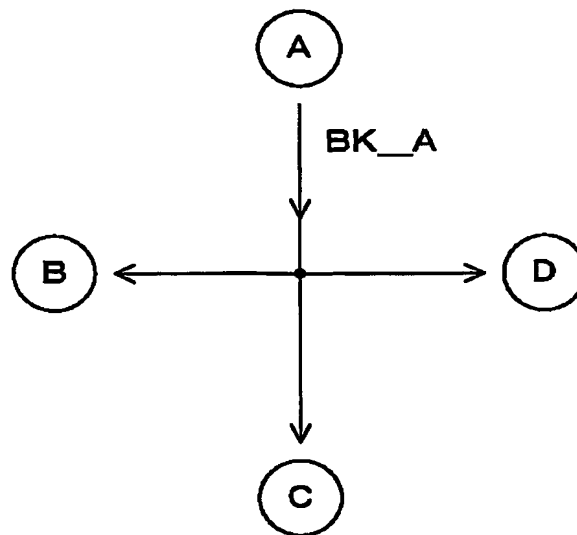
端末識別子                  ユニキャスト暗号鍵                  ブロードキャスト暗号鍵

端末B	UK_AB	BK_B
端末C	UK_AC	BK_C
端末D	UK_AD	BK_D

Fig.5

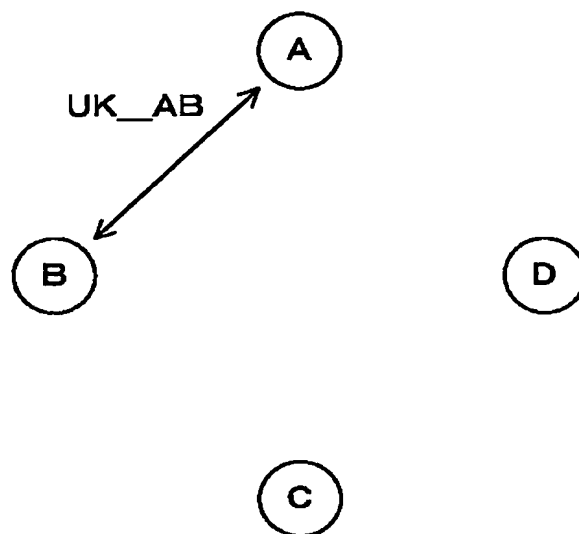
6/17

Fig.6A



ブロードキャスト鍵

Fig.6B



ユニキャスト鍵

7/17

680 ↙

681 終点端末識別子	682 転送先端末識別子	683 有効時間
端末B	端末B	1:30
端末C	端末B	0:50
端末D	端末B	0:30
⋮	⋮	⋮

Fig.7

8/17

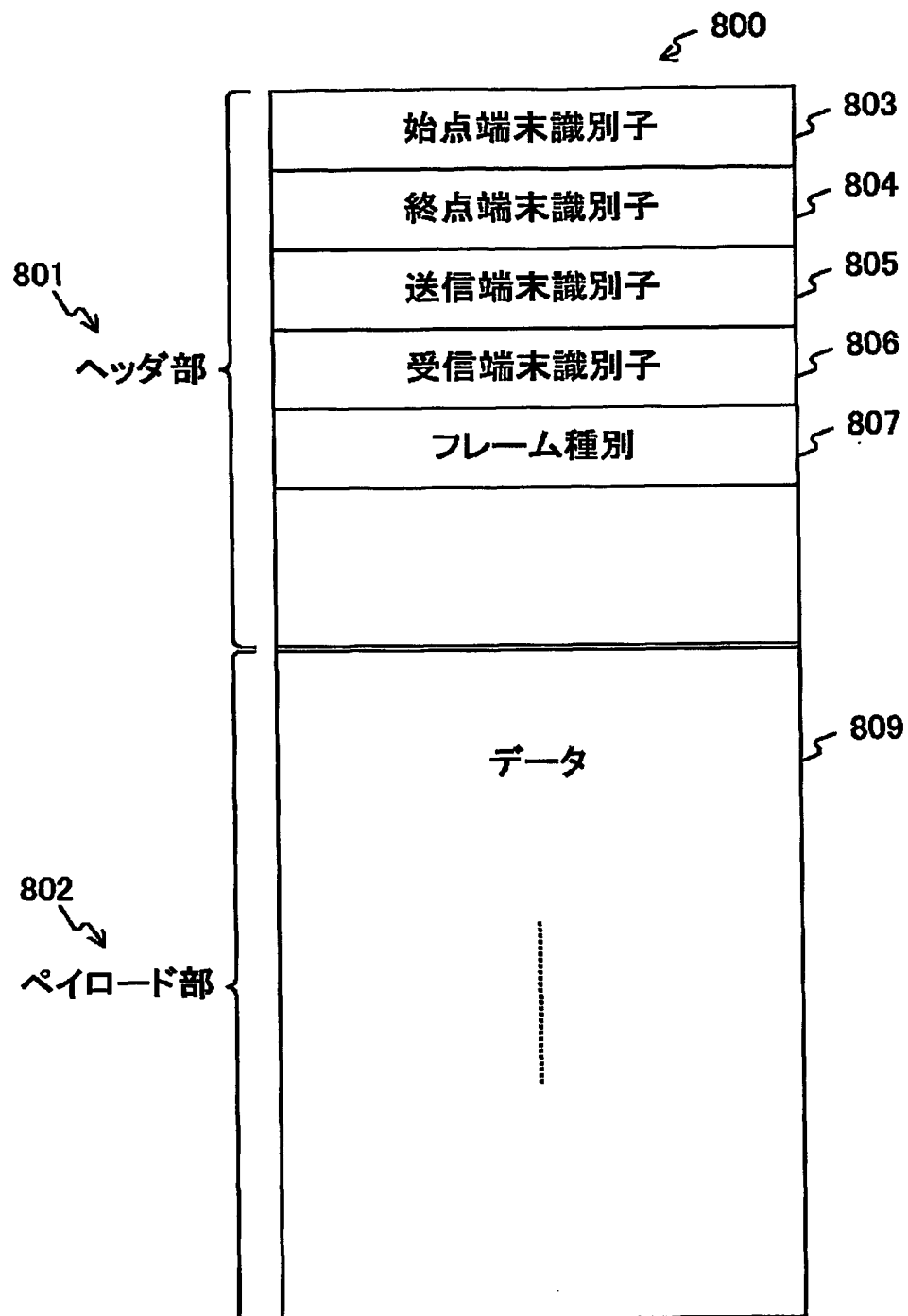


Fig.8

9/17

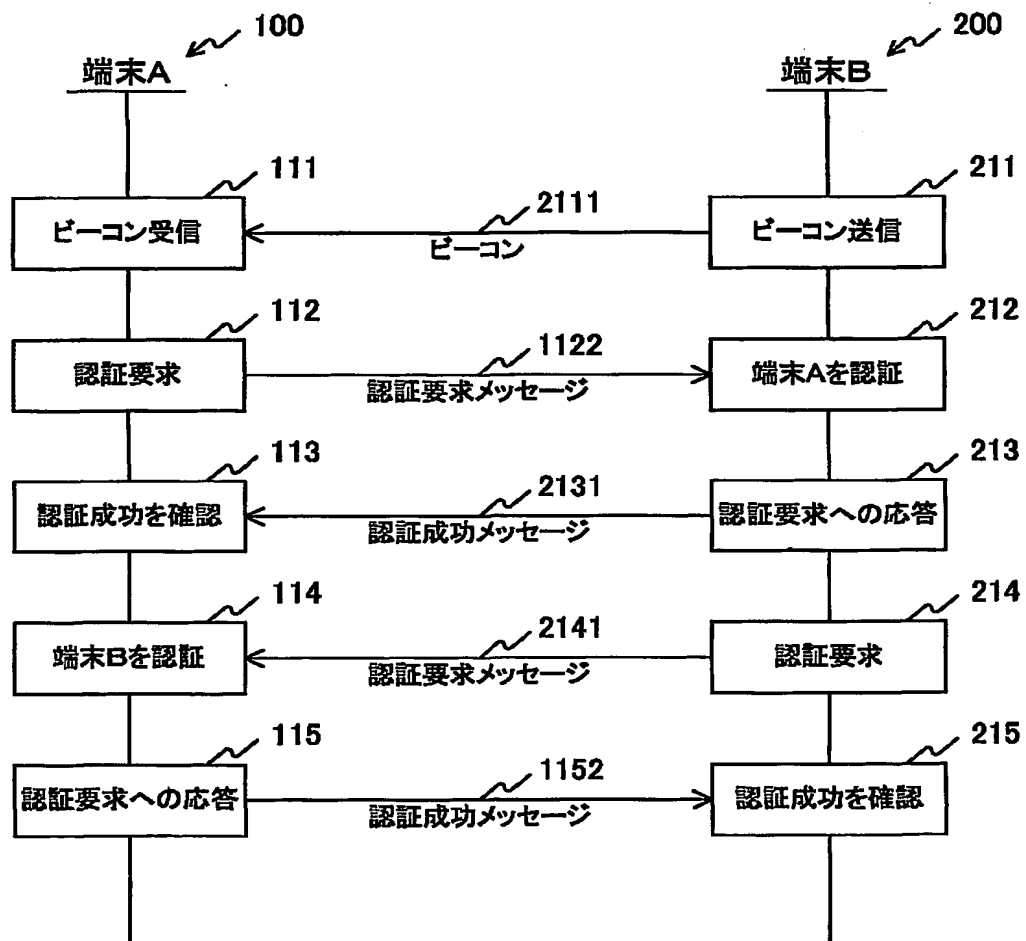


Fig.9

10/17

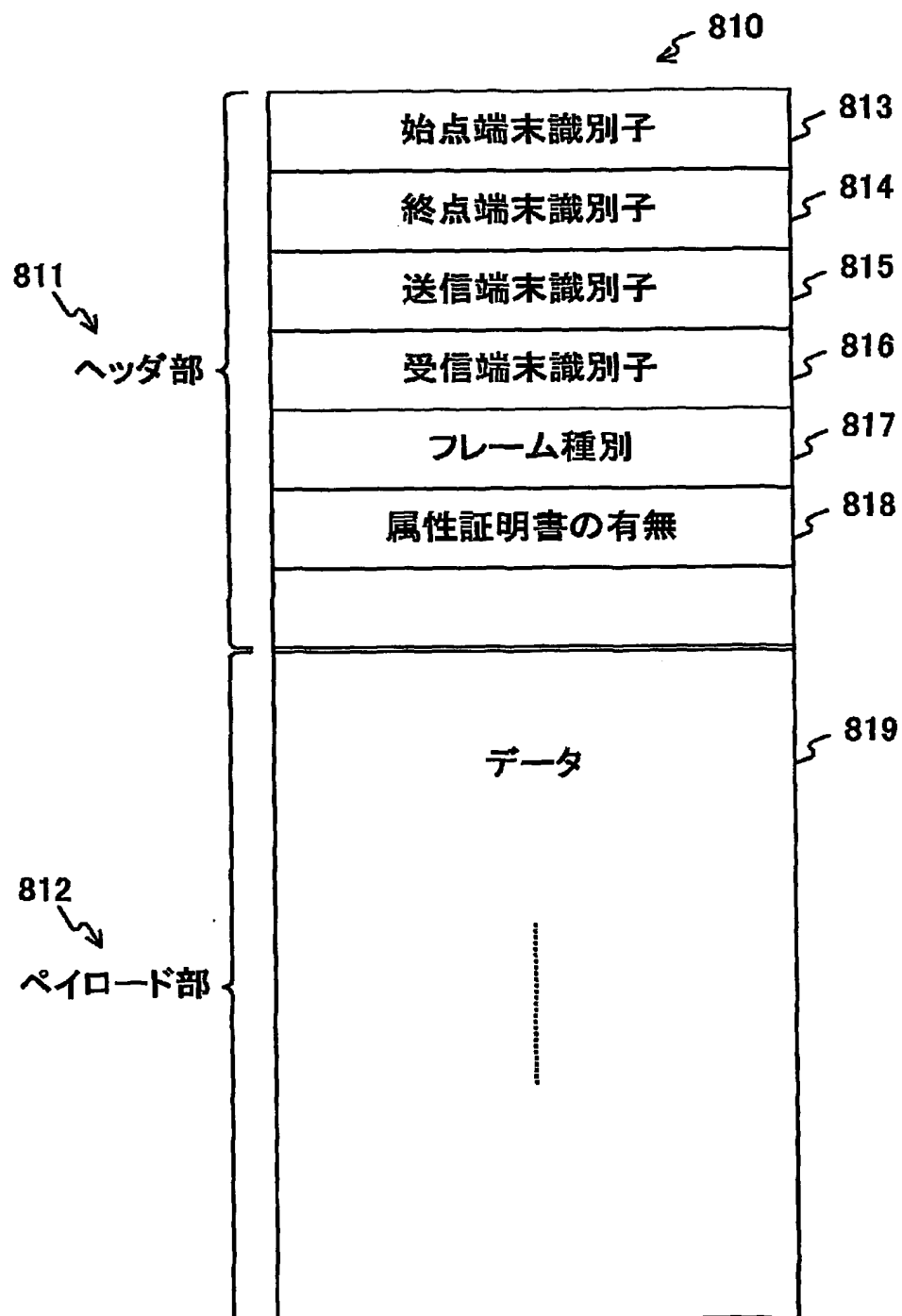


Fig.10

11/17

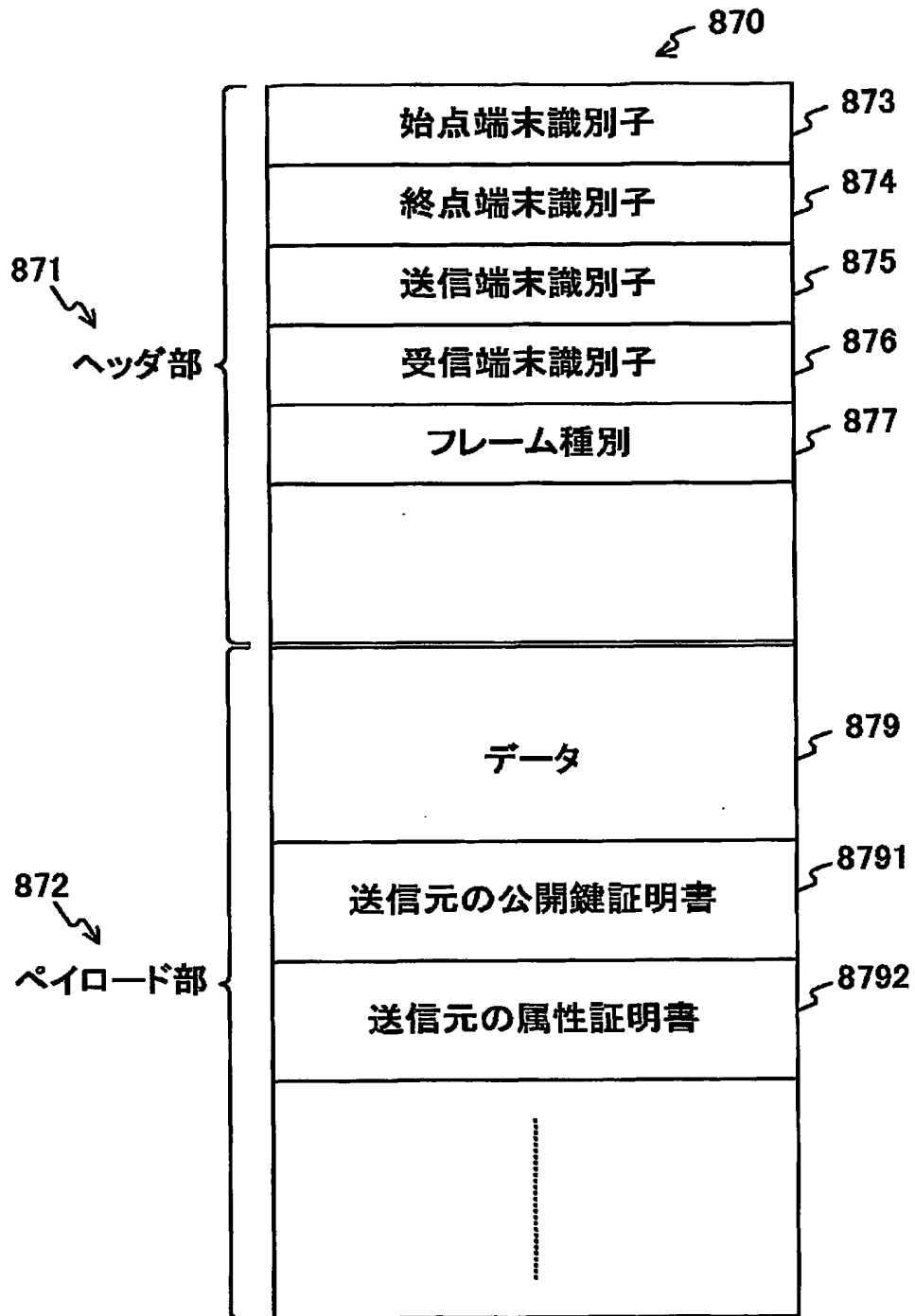


Fig.11

12/17

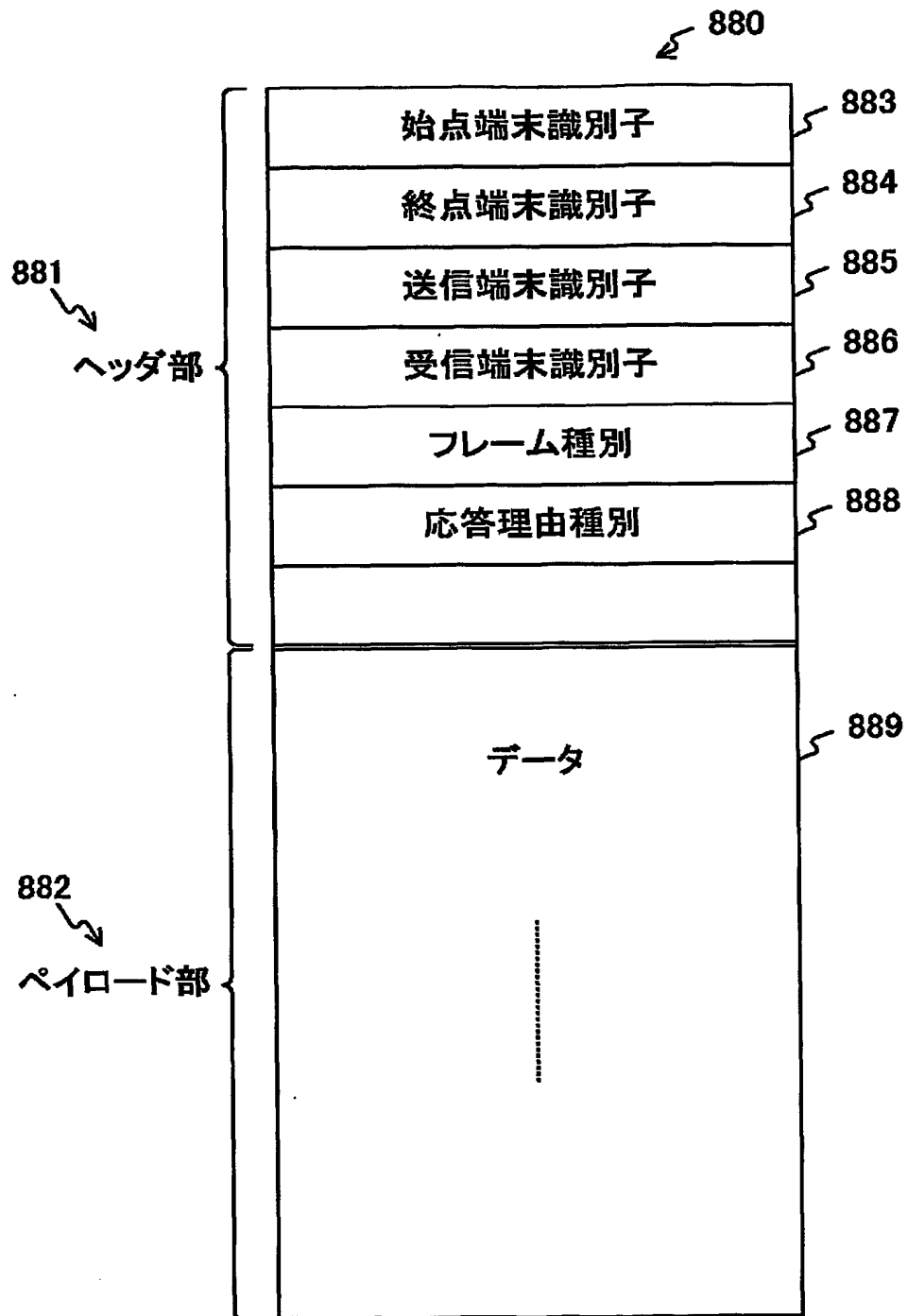


Fig.12



13/17

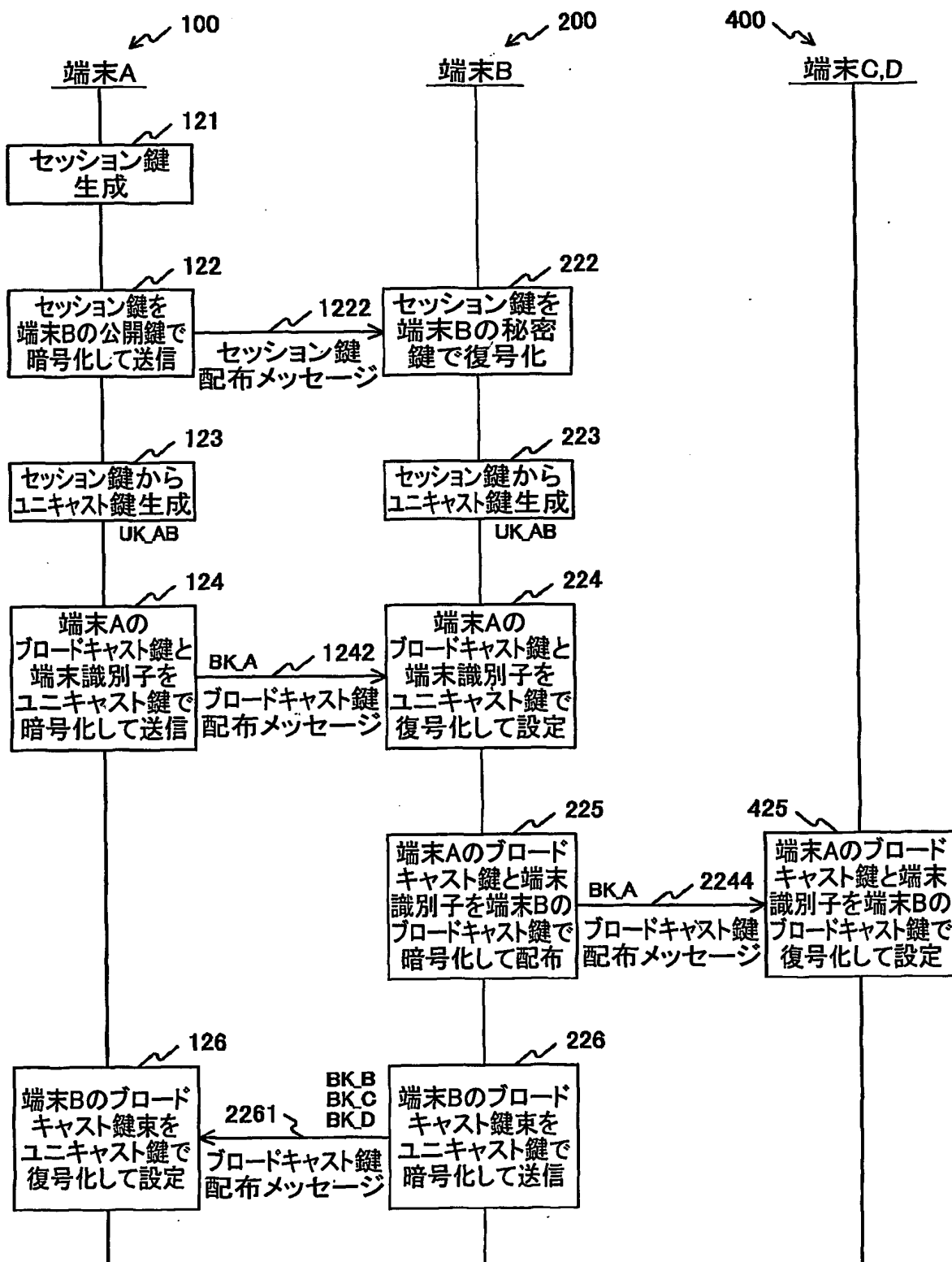


Fig.13

14/17

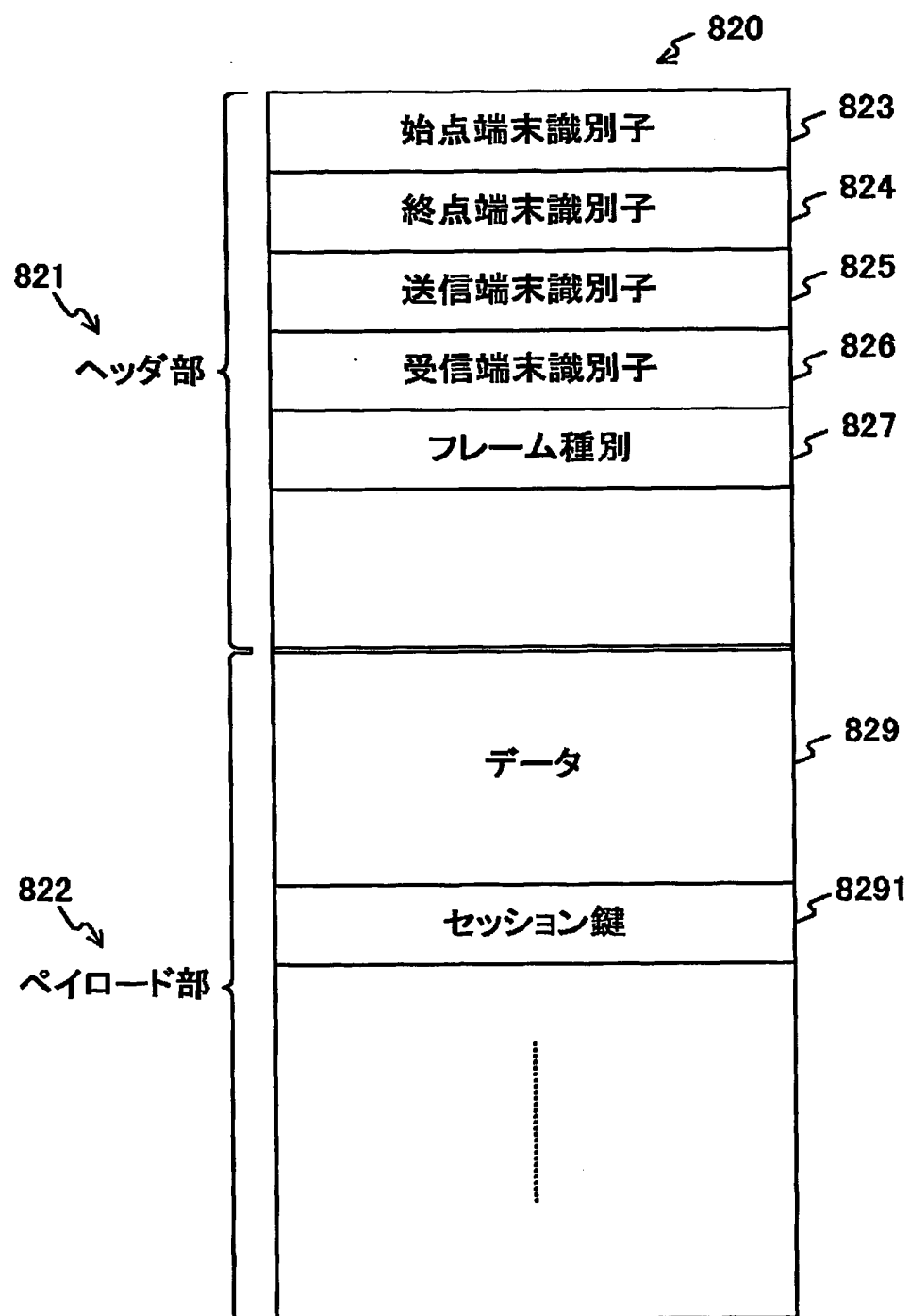


Fig.14

15/17

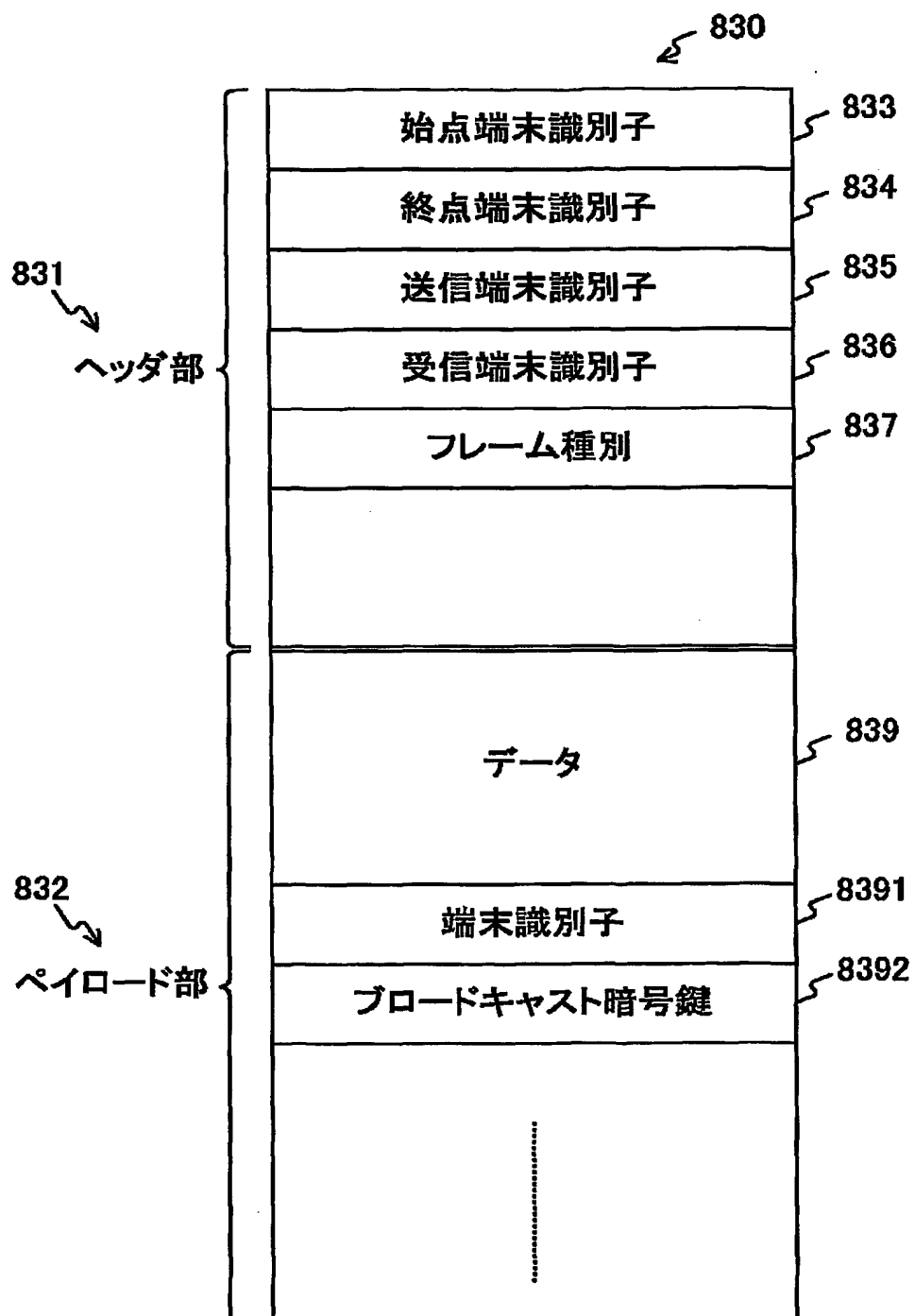


Fig.15

16/17

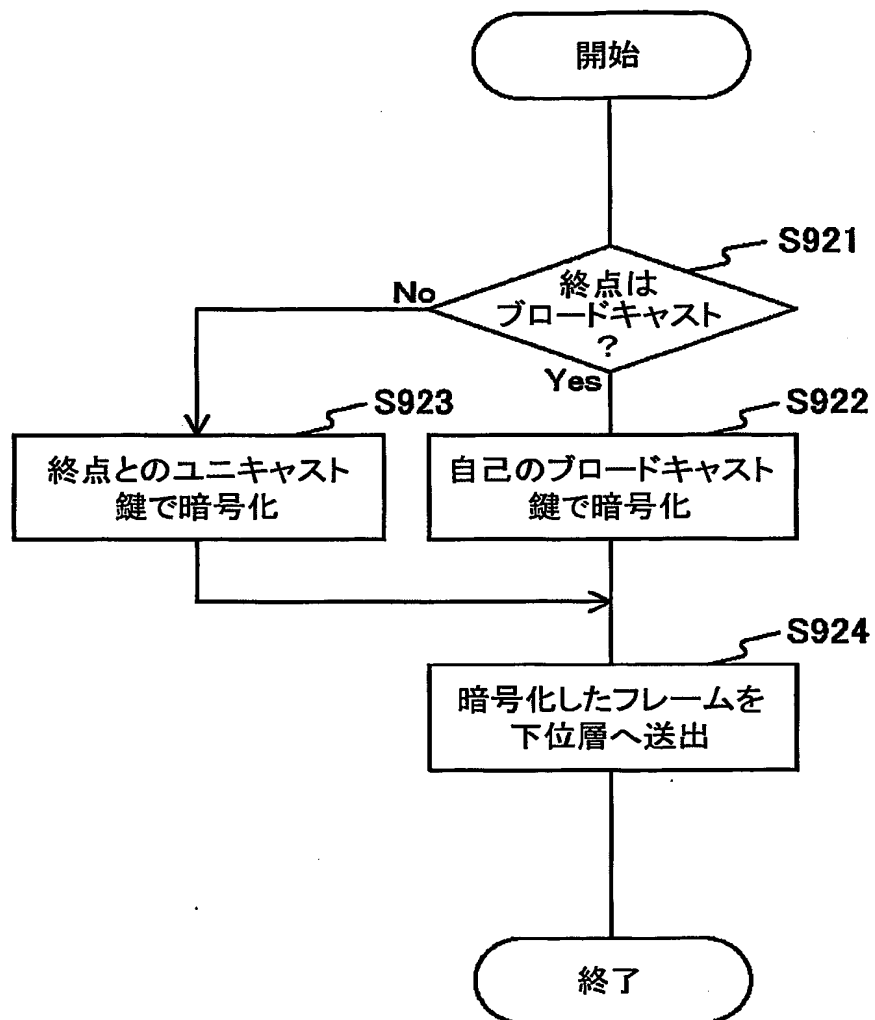


Fig.16

17/17

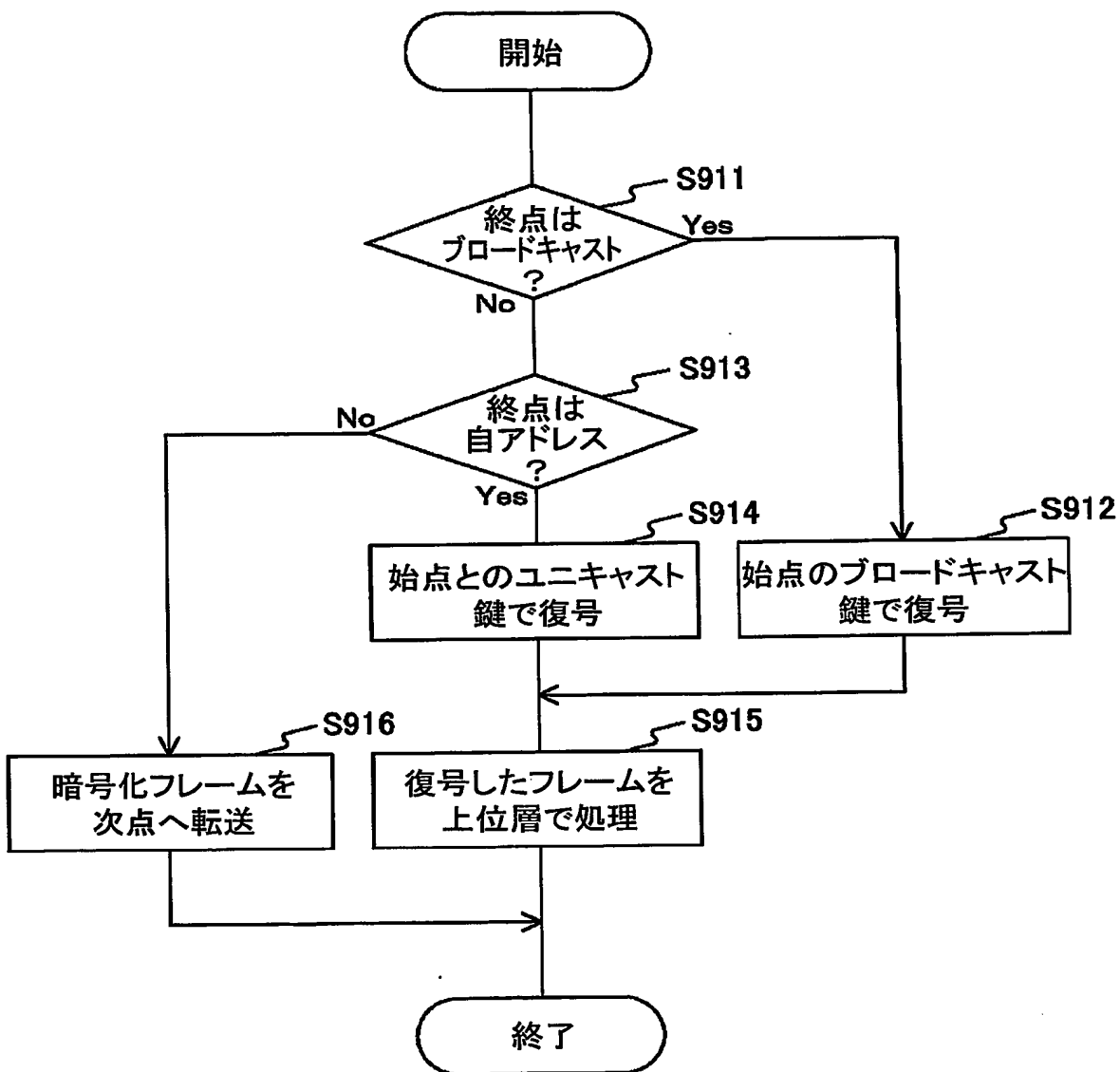


Fig.17